

Presentingpartner

K Y O S

Goldsponsor



www.leaderdigital  
www.digitalconference.ch  
August 6 | 2026 | CHF 5



# Digital Conference Ostschweiz

Die LEADER-Sonderausgabe zum Event am  
8. September 2026 im Einstein Congress, St.Gallen



Organisation

<IT>rockt! LEADER east#digital





# CAS Angewandte KI im Business

## CAS KI im Marketing

- CAS-Abschluss (Certificate of Advanced Studies) in Kooperation mit der Hochschule HSSH
- 15 ECTS-Punkte
- 6 Monate berufsbegleitend
- CHF 9'900.– all-inclusive
- Start November 2026

- KI erfolgreich im Unternehmen einsetzen
- Prozesse automatisieren
- Produktivität steigern
- Marketing revolutionieren

Hybrid,  
vor Ort  
oder  
online.



**BVS** St Gallen



bvs.ch

# KI und Cybersecurity gemeinsam denken – willkommen zur Digital Conference Ostschweiz 2026

**Die** Digital Conference Ostschweiz hat sich als führender Treffpunkt für Digitalisierung in der Ostschweiz etabliert. Es freut mich, dass LEADER, east#digital und <IT>rockt! auch 2026 wieder gemeinsam eine Plattform schaffen, auf der sich Unternehmer, IT-Verantwortliche und Entscheidungsträger über die wichtigsten Entwicklungen austauschen können.

Das diesjährige Motto lautet: «Cybersecurity trifft KI: Risiko oder Chance?». Kaum ein Thema beschäftigt Unternehmen derzeit stärker. Künstliche Intelligenz eröffnet neue Möglichkeiten, verändert Geschäftsmodelle und steigert die Effizienz. Gleichzeitig entstehen neue Herausforderungen für Sicherheit, Datenschutz und Vertrauen. Wer die Chancen nutzen will, muss auch die Risiken verstehen.

Genau hier setzt die DCONO an. Hochkarätige Referenten vermitteln aktuelles Wissen, praxisnahe Breakout-Sessions liefern konkrete Lösungsansätze und zahlreiche Networking-Möglichkeiten fördern den Austausch zwischen Wirtschaft, Wissenschaft und IT-Branche. Nutzen Sie diese Gelegenheit, um neue Impulse mitzunehmen und wertvolle Kontakte zu knüpfen.

Mein herzlicher Dank gilt unseren Partnern und Sponsoren, die diese Veranstaltung ermöglichen. Ich wünsche Ihnen eine spannende Lektüre dieses Vorschau-Specials und freue mich darauf, Sie am 8. September 2026 im Einstein Congress St.Gallen persönlich begrüßen zu dürfen.

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 erhalten Sie einen ersten Einblick in die Digital Conference Ostschweiz 2026. Die Digitalisierung entwickelt sich rasant weiter. Insbesondere Künstliche Intelligenz verändert Prozesse, Produkte und Dienstleistungen in einer Geschwindigkeit, die viele Unternehmen vor neue strategische Entscheidungen stellt. Gleichzeitig nehmen Cyberbedrohungen weiter zu. Beides lässt sich heute nicht mehr getrennt betrachten.

Die DCONO bringt deshalb Fachleute, Unternehmer und Entscheidungsträger zusammen, um Chancen und Risiken gemeinsam zu diskutieren. Renommierte Referenten zeigen aktuelle Entwicklungen auf, Breakout-Sessions liefern praxisnahe Einblicke und konkrete Lösungsansätze für den Unternehmensalltag. Gleichzeitig bietet die Konferenz zahlreiche Möglichkeiten, Erfahrungen auszutauschen und das persönliche Netzwerk zu erweitern.

Die Ostschweiz verfügt über einen starken und innovativen ICT-Standort. Mit der Digital Conference Ostschweiz möchten wir dazu beitragen, dieses Netzwerk weiter zu stärken und den Wissenstransfer zwischen Unternehmen, Forschung und Praxis zu fördern.

Ich wünsche Ihnen eine interessante Lektüre und freue mich, Sie am 8. September 2026 im Einstein Congress St.Gallen persönlich willkommen zu heissen.

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

# Sponsoren und Partner

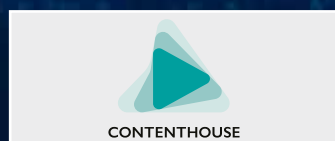
## Presentingpartner



## Goldpartner



## Silberpartner



## Bronzepartner



## Netzwerkpartner



## Award-Sponsor



## Hostpartner



## Impressum

**Magazin LEADER, MetroComm AG, Bahnhofstrasse 8, 9000 St.Gallen, T 071 272 80 50, 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, Rebecca Grossglauser, zVg | **Gestaltung:** Doris Hollenstein, Beatrice Lang | **Herausgeberin, Redaktion und Verlag:** MetroComm AG, Bahnhofstrasse 8, 9000 St.Gallen, T 071 272 80 50, 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.

LEADER ist ein beim Institut für geistiges Eigentum eingetragenes Markenzeichen. Nachdruck, auch auszugsweise, nur mit schriftlicher Genehmigung des Verlages. Für unverlangt eingesandte Manuskripte übernimmt der Verlag keine Haftung. ISSN 1660-2757



# Do it in St.Gallen!

**Die** Digital Conference Ostschweiz findet in St.Gallen statt – und damit an einem Ort, der Tradition und Zukunft auf einzigartige Weise verbindet. Als Wirtschafts- und Bildungsstandort mit internationaler Ausstrahlung, geprägt durch die Universität St.Gallen, ein dynamisches Unternehmertum und eine wachsende Innovationsszene, bietet unser Kanton ideale Voraussetzungen für den Dialog über die digitale Transformation unserer Gesellschaft.

Die Ostschweiz hat starke KMU, industrielle Kompetenz und eine hohe Exportorientierung. Gerade deshalb ist der Austausch zwischen Entscheidungsträgern, ICT-Spezialisten, Forschenden und Wirtschaftsvertretern von zentraler Bedeutung. Die Digital Conference leistet hierzu einen wertvollen Beitrag: Sie stärkt das regionale Tech-Ökosystem, fördert Kooperationen und positioniert die Ostschweiz als Hub für Innovation und digitale Wertschöpfung.

Beat Tinner, Regierungsrat,  
Vorsteher Volkswirtschafts-  
departement Kanton St.Gallen



Das diesjährige Thema rückt die Chancen und Herausforderungen von Künstlicher Intelligenz und Cybersicherheit in den Fokus. Diese Entwicklungen verändern Wirtschaft und Gesellschaft grundlegend. Der Kanton St.Gallen verfolgt eine klare Strategie: Wir fördern den verantwortungsvollen Einsatz von KI, stärken die digitale Kompetenz in Unternehmen und Verwaltung und setzen uns zugleich für hohe Sicherheitsstandards im Umgang mit Daten und Infrastrukturen ein. Cybersicherheit ist für uns eine Voraussetzung für Vertrauen – und damit für nachhaltige Innovation.

St.Gallen steht für Offenheit, kurze Wege, Qualität und Vernetzung. Wir sind der beste Standort für innovative Köpfe und

ihre Projekte. Ich bin überzeugt, dass von dieser Konferenz wichtige Impulse ausgehen werden – für die Region und darüber hinaus.

Im Namen der Regierung des Kantons St.Gallen wünsche ich allen Teilnehmenden inspirierende Begegnungen und erkenntnisreiche Diskussionen. <

## Anfahrt, Programm und Tickets

### Adresse

Einstein Congress  
Wassergasse 3  
9000 St.Gallen

### 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.

### Programm

Hier finden Sie das detaillierte Programm >>



### Tickets

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



# Cybersecurity trifft KI: Die Zukunft beginnt jetzt

Künstliche Intelligenz eröffnet Unternehmen enorme Chancen, verändert aber gleichzeitig die Anforderungen an Sicherheit, Führung und Vertrauen. Genau diesem Spannungsfeld widmet sich die Digital Conference Ostschweiz 2026. Am 8. September treffen sich im Einstein Congress St.Gallen Entscheidungsträger aus Wirtschaft, Verwaltung und IT, um über die Zukunft von KI, Cybersecurity und digitaler Transformation zu diskutieren.

Bereits zum vierten Mal bringen <IT>rockt!, das Unternehmermagazin LEADER und east#digital führende Persönlichkeiten aus Wissenschaft, Wirtschaft und Politik auf einer Bühne zusammen. Unter dem Motto «Cybersecurity trifft KI – Risiko oder Chance?» stehen nicht theoretische Zukunftsszenarien im Mittelpunkt, sondern konkrete Erfahrungen, praxisnahe Lösungsansätze und der persönliche Austausch.

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

## Hochkarätige Impulse

Mit **Richard David Precht**, Philosoph und Publizist, konnte einer der bekanntesten Denker des deutschsprachigen Raums als Keynote-Speaker gewonnen werden. Gemeinsam mit **Jill Wick**, Wirtschaftspsychologin und Security-Awareness-Expertin, **Anna-Lena Horlemann**, Professorin für theoretische Informatik und Mathematik an der HSG, sowie **Henriette Engbersen**, Leiterin Public Value bei der

SRG, beleuchten die Referenten das Leitthema aus unterschiedlichen Perspektiven. Im Fokus stehen die gesellschaftlichen Auswirkungen der künstlichen Intelligenz, ihr verantwortungsvoller Einsatz in Unternehmen, die Verbindung von KI und Cybersecurity sowie der Umgang mit Desinformation und Vertrauen.

## «Die Digital Conference lebt von ihrer Praxisnähe.»

«Die Brisanz der Thematik hat sich durch KI in den letzten Jahren deutlich verschärft», sagt Henriette Engbersen. Ergänzt wird das Programm durch einen Regierungsimpuls von **Beat Tinner**, Vorsteher des Volkswirtschaftsdepartements des Kantons St.Gallen.

## Praxiswissen für Unternehmen

Neben den Keynotes bietet die Digital Conference Ostschweiz fünf Breakout-Sessions, in denen Experten aus Wirtschaft und IT konkrete Erfahrungen und Lösungsansätze vorstellen. Die Themen reichen von Cyber Resilience und KI-

Sicherheit über Datenstrategie und Compliance bis hin zu Incident Response und dem Faktor Mensch. Im Mittelpunkt stehen praxisnahe Beispiele und Handlungsempfehlungen, die Unternehmen direkt in ihren Arbeitsalltag übernehmen können.

«Man muss kein gezieltes Angriffsziel sein, um Opfer eines Cyberangriffs zu werden», sagt Sylvain Luiset, Head of Cyber Resilience Consulting Switzerland bei Zurich Insurance. Seine Breakout-Session zeigt, weshalb Cybersecurity heute weit mehr als ein IT-Thema ist und wie Unternehmen ihre Widerstandsfähigkeit gezielt stärken können.





## «Digitalisierung gelingt nicht im Alleingang.»

### Wissen teilen und Netzwerke pflegen

Neben den Referaten bietet die Digital Conference Ostschweiz zahlreiche Gelegenheiten zum persönlichen Austausch. Unternehmer, Verwaltungsräte, Geschäftsleitungsmitglieder, IT-Verantwortliche und Digitalisierungsexperten diskutieren aktuelle Herausforderungen, teilen Erfahrungen und knüpfen neue Kontakte.

«Digitalisierung gelingt nicht im Alleingang. Sie braucht das Zusammenspiel unterschiedlicher Akteure aus Wirtschaft, Verwaltung, Forschung und IT», sagt Eva De Salvatore, Geschäftsführerin von <IT>rockt!.

Ein weiterer Programmhöhepunkt ist die Auszeichnung **Digital Shaper Ostschweiz 2026**. Geehrt werden Persönlichkeiten und Teams, die mit ihren Ideen und Projekten die digitale Entwicklung der Region nachhaltig prägen.

### Jetzt Ticket sichern

Ob künstliche Intelligenz, Cybersecurity oder digitale Transformation: Die Digital

Conference Ostschweiz 2026 bietet aktuelle Erkenntnisse, konkrete Praxisbeispiele und wertvolle Kontakte für alle, die die digitale Zukunft ihres Unternehmens aktiv mitgestalten wollen. <

Das vollständige Programm, Speaker-Infos und Anmeldung: [digitalconference.ch](https://digitalconference.ch)





# «Hier wird Innovation gelebt»

Cyberangriffe, künstliche Intelligenz und immer mehr regulatorische Anforderungen stellen Unternehmen vor immer schwierigere Entscheidungen. Andy Kutter, Direktor der Kyos SA am Standort St.Gallen, weiss, weshalb Cybersecurity in die Chefetage gehört, wie Sicherheit zum Wettbewerbsvorteil wird und welche Chancen er für den Digitalstandort Ostschweiz sieht.

Andy Kutter, Kyos engagiert sich seit Jahren an der Digital Conference Ostschweiz und hat dieses Engagement 2026 langfristig ausgebaut. Weshalb ist Ihnen die Veranstaltung wichtig?

Die Digital Conference Ostschweiz zeigt jedes Jahr, wie viel Innovationskraft in unserer Region steckt. Für mich ist sie eine der wichtigsten Plattformen für Menschen, die deren Zukunft aktiv mitgestalten. Unsere Stärke liegt in den innovativen Unternehmen, den starken Bildungsinstitutionen und den kurzen Wegen. Man begegnet sich, tauscht sich aus und entwickelt Ideen. Die DCONO bringt diese Qualitäten zusammen und schafft einen Austausch, der über die Veranstaltung hinauswirkt. Deshalb engagieren wir uns mit Überzeugung!

Cybersecurity ist längst kein reines IT-Thema mehr. Welche Denkfehler beobachten Sie bei Geschäftsleitungen und Verwaltungsräten am häufigsten? Die Annahme, Cybersecurity lasse sich wie ein Investitionsprojekt behandeln: Wir setzen die notwendigen Massnahmen um und sind danach sicher. Tatsächlich ist sie eine permanente

Managementaufgabe. Bedrohungslage, Technologien, Geschäftsmodelle und Risiken verändern sich laufend. Oft lautet die Frage immer noch: Wie gross ist die Wahrscheinlichkeit, dass es uns trifft? Entscheidender aber wäre: Wie gut sind wir vorbereitet, wenn es uns trifft? Absolute Sicherheit gibt es zwar nicht, aber man kommt nahe dran, wenn man es richtig aufgleist. Deshalb gehört Cybersecurity in die Verantwortung von Geschäftsleitung und Verwaltungsrat. Es geht um Resilienz, Risikomanagement und die langfristige Handlungsfähigkeit des Unternehmens.

## «Gute Cybersecurity muss nicht teuer sein.»

KI verändert die Bedrohungslage und die Erwartungen der Kunden. Wie hat sich Ihre Rolle als Berater und Sparringspartner dadurch verändert?

Nicht grundsätzlich, die Fragen unserer Kunden haben sich aber erweitert. Cybersecurity, Risikomanagement und

Governance standen schon immer im Zentrum. Mit KI kommen aber weitere Themen hinzu.

### Welche?

Früher ging es häufig darum, Systeme zu schützen oder regulatorische Anforderungen zu erfüllen. Heute diskutieren wir darüber, wie sich neue Technologien verantwortungsvoll einsetzen lassen, welche Risiken entstehen und wie Unternehmen die Kontrolle über Daten, Prozesse und Entscheidungen behalten. KI ist dabei ein wichtiger Treiber, aber nicht der einzige. Denn Cybersecurity, Compliance, Datenmanagement und KI





lassen sich kaum noch isoliert betrachten. Unsere Aufgabe besteht zunehmend darin, diese Themen ganzheitlich einzuordnen und Unternehmen bei fundierten Entscheidungen zu unterstützen.

**Cybersecurity gilt für viele Unternehmen noch immer als reiner Kostenfaktor ...**

Leider! Viele Unternehmen unterschätzen auch, wie stark Cybersecurity zu ihrer Wahrnehmung beiträgt. Niemand entscheidet sich zwar allein wegen der Security für einen Anbieter. Wird sie aber vernachlässigt, geht Vertrauen schnell verloren. Und: Gute Cybersecu-

ty muss nicht zwangsläufig teuer sein. Entscheidend ist, Risiken zu verstehen und bewusst zu managen. Wer verantwortungsvoll mit Daten umgeht und auf den Ernstfall vorbereitet ist, hebt sich positiv von Mitbewerbern ab. So wird Cybersecurity zum Wettbewerbsvorteil.

**Technologien entwickeln sich rasant. Wie entscheidet Kyos, welche Trends für Kunden relevant sind?**

Wir bewerten neue Technologien nicht nach der Aufmerksamkeit, die sie erhalten, sondern nach dem Problem, das sie lösen. Neu bedeutet noch lange nicht

**«Neu bedeutet noch lange nicht relevant.»**

relevant. Viele Technologien durchlaufen ja einen Hypezyklus. Deshalb fragen wir: Verbessert eine Lösung die Sicherheit oder Effizienz? Reduziert sie Risiken? Oder erzeugt sie zusätzliche Komplexität? Unsere Kunden interessiert nicht, welche Technologie morgen Schlagzeilen macht, sondern welche ihrem Unternehmen konkreten Mehrwert bringt. >



> **Vertrauen ist in Ihrer Branche entscheidend. Weshalb überlassen Kunden Kyos ihre kritischsten Systeme?**

Vertrauen ist keine Frage von Versprechen, sondern von Glaubwürdigkeit. Kunden wissen, dass wir ihre Interessen in den Mittelpunkt stellen und nicht jene eines Herstellers oder einer bestimmten Lösung. Wir beurteilen Risiken objektiv und empfehlen, was fachlich und wirtschaftlich sinnvoll ist. Es geht nicht um möglichst viel Technologie, sondern um die richtige Lösung. Vertrauen zeigt sich nicht in dem, was wir über uns sagen, sondern in dem, was Kunden uns anvertrauen. Dass Unternehmen aus unterschiedlichsten Branchen ihre kritischen Systeme, Sicherheitsstrategien und sensibelsten Fragen in unsere Hände geben, ist für mich die stärkste Bestätigung unserer Arbeit.

**Welche Führungsprinzipien haben sich in einer Branche bewährt, in der sich Technologien laufend verändern und Vertrauen die wichtigste Währung ist?** Unser Organisationsmodell basiert auf Vertrauen, Eigenverantwortung und Fachkompetenz. Das prägt mein Füh-

rungsverständnis. Die besten Entscheidungen entstehen nicht zwangsläufig auf der höchsten Hierarchiestufe; in einer Wissensbranche haben oft die Menschen mit der grössten Expertise die besten Antworten. Meine Aufgabe ist weniger, Entscheidungen vorzugeben, als die richtigen Rahmenbedingungen zu schaffen, damit Menschen Verantwortung übernehmen und ihr Potenzial entfalten. Zum Erfolgsfaktor wird nicht Kontrolle, sondern die Fähigkeit, Wissen zu teilen, voneinander zu lernen und Verantwortung dort wahrzunehmen, wo die Kompetenz liegt.

**«Es geht nicht um möglichst viel Technologie, sondern um die richtige Lösung.»**

**Wo sehen Sie die grössten Chancen, den Digitalstandort Ostschweiz in den kommenden Jahren weiterzuentwickeln?**

Die Ostschweiz muss nicht das nächste Zürich oder Silicon Valley werden. Ihre

Stärke liegt darin, dass sie anders ist. Innovative Unternehmen, starkes Unternehmertum und eine Kultur der Umsetzung prägen die Region. Hier wird Innovation täglich gelebt. Aber: Wir sollten Wissen aus Forschung und Bildung noch besser mit den Bedürfnissen der Wirtschaft verbinden und neue Technologien schneller in die Praxis bringen. Die Zukunft des Digitalstandorts entscheidet sich nicht daran, wer die meisten Ideen hat, sondern daran, wer die besten erfolgreich umsetzt.

**Welche Weichen müssen Unternehmen heute stellen, damit sie in fünf Jahren digital erfolgreich sind?**

Die nächsten fünf Jahre werden viele Unternehmen stärker fordern als die vergangenen. Mehrere Entwicklungen kommen gleichzeitig zusammen: KI, neue regulatorische Anforderungen, steigende Ansprüche an Daten, Zugriffsrechte und Cloud-Dienste sowie mittelfristig die Post-Quanten-Kryptografie. Unternehmen müssen ihre digitale Grundlage also sauber aufstellen. Sie müssen wissen, wo kritische Daten liegen, wer darauf zugreifen kann, welche Prozesse zentral sind und von welchen Systemen oder Partnern sie abhängen. Sonst wird es schwierig, neue Anforderungen schnell und sicher umzusetzen. Das gilt für regulatorische Vorgaben ebenso wie für kürzere Zertifikatslaufzeiten, neue kryptografische Verfahren oder den sinnvollen Einsatz von KI.

**Viele werden wohl aber warten, bis der Druck gross genug ist ...**

Ja, aber erfolgreich werden jene Unternehmen sein, die sich frühzeitig auf Entwicklungen vorbereiten, die heute noch technisch oder weit entfernt wirken. So schaffen sie sich den Handlungsspielraum, den andere erst aufbauen müssen. <



# Die Moderatorin der DCONO 2026



Bild: Mirjam Kluka

[bignasilberschmidt.ch](https://bignasilberschmidt.ch)

 [bigna-silberschmidt-20b972a9](https://www.instagram.com/bigna-silberschmidt-20b972a9)

 [bignasilberschmidt](https://www.linkedin.com/company/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 und Print war Bigna Silberschmidt während zehn Jahren beim Schweizer Fernsehen SRF als Reporterin und Moderatorin tätig. Sie realisierte Dokumentarfilme und

zahlreiche Reportagen und moderierte «Schweiz aktuell», das Wissensmagazin «Einstein» sowie zuletzt die Informationssendung «10 vor 10».

2025 machte sich die Journalistin mit der SilberMedia GmbH selbstständig. Bigna Silberschmidt moderiert Podien und Veranstaltungen in den Bereichen Wissenschaft, Gesellschaft, Umwelt und Wirtschaft, berät inhaltlich und konzeptionell und hält Referate. Zudem doziert sie im Bereich konstruktive und inklusive Kommunikation.

Anzeige

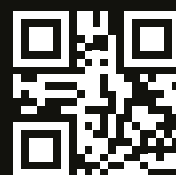


**acreo  
consulting**  
partnering  
transformation

[acreo.ch](https://acreo.ch)

# Wir machen Schluss ...

Mehr dazu:  
Breakout-Session 2  
15.00 Uhr







# Precht stellt der KI die Menschenfrage

Richard David Precht gehört zu den bekanntesten (und streitbarsten) Intellektuellen im deutschsprachigen Raum. An der Digital Conference Ostschweiz wirft der Keynote-Speaker einen etwas anderen Blick auf die Künstliche Intelligenz.

Richard David Precht ist kein Philosoph für den akademischen Elfenbeinturm. Er sucht die Öffentlichkeit, mischt sich in gesellschaftliche Debatten ein und formuliert so pointiert, dass seine Aussagen weit über Fachkreise hinaus Beachtung finden.

Der wöchentliche ZDF-Podcast «Lanz + Precht» hat allein auf Spotify weit über 100 Millionen Streams und erhielt dafür etwa den «Creator Milestone Award» in Bronze.

**Precht gehört zu den wenigen prominenten deutschen Intellektuellen, die öffentlich Klartext reden**

Er scheut den Widerspruch nicht und nimmt in Kauf, anzuecken. Das macht ihn für die einen zum Impulsgeber und für die anderen zur Reizfigur. Gleichgültig lässt er sein Publikum kaum.

Geboren wurde Precht 1964 in Solingen. Er studierte Germanistik, Philosophie und Kunstgeschichte an der Universität Köln; seit 2012 ist er Honorarprofessor für Philosophie und Ästhetik an der Hochschule für Musik Hanns Eisler Berlin.

Einem breiten Publikum wurde er mit «Wer bin ich – und wenn ja, wie viele?» bekannt. Seine Bücher wurden in mehr als 40 Sprachen übersetzt. Seit 2012 moderiert er zudem die ZDF-Gesprächsreihe «Precht», die im Mai 2026 ihre 84. Ausgabe erreichte.

**Mit künstlicher Intelligenz beschäftigt sich Precht nicht erst seit ChatGPT**

Bereits 2020 veröffentlichte er den Essay «Künstliche Intelligenz und der Sinn des Lebens». Darin stellt er weniger die Leistungsfähigkeit von Maschinen als deren gesellschaftliche und philosophische Grenzen ins Zentrum. Seine entscheidende Frage lautet nicht nur, was KI kann, sondern was Menschen ihr überlassen wollen.

**«Wir kürzen aus der Welt der Erkenntnis den menschlichen Faktor raus»**

Menschliches Leben besteht für Richard David Precht nicht allein aus dem Lösen von Problemen. Es ist ebenso mit Erfahrung, Emotion, Sinn und moralischer Verantwortung verbunden.

Am 9. Juli 2026 griff er diese Gedanken in der Podcastfolge «Ist der KI-Hype am Ende?» erneut auf. Precht warnte dort vor den Folgen, wenn Menschen Erkenntnisprozesse zunehmend an Maschinen delegieren. «Wir kürzen aus der Welt der Erkenntnis den menschlichen Faktor raus», sagt er.

Seine Sorge gilt einer Kultur, in der lange

Richard David Precht  
Philosoph, Publizist und  
Bestsellerautor

In seiner Keynote richtet Precht den Blick weniger auf technische Details als auf die Frage, wie künstliche Intelligenz unser Zusammenleben verändert. Er zeigt auf, welche Folgen automatisierte Entscheidungen für Arbeit, Verantwortung und gesellschaftliche Machtverhältnisse haben und wo Wirtschaft, Politik und Gesellschaft Grenzen setzen müssen. Dabei beleuchtet er sowohl Chancen für Innovation und Produktivität als auch Risiken für Selbstbestimmung, Bildung und demokratische Kontrolle.

Texte nicht mehr gelesen, sondern nur noch durch KI zusammengefasst werden. Damit könnten Neugier, gedankliche Ausdauer und die Bereitschaft schwinden, sich ein eigenes Urteil zu erarbeiten. Zugleich fragt er, ob wenige Technologiekonzerne mit dem Wissen und den Werken der gesamten Menschheit Milliarden Geschäfte machen dürfen.

**Für die Wirtschaft ist diese Perspektive unbequem, aber produktiv**

KI kann Prozesse beschleunigen, Routinen übernehmen und Mitarbeiter entlasten. Effizienz beantwortet jedoch nicht, wie Arbeit künftig verteilt, Verantwortung zugeordnet und soziale Sicherheit organisiert werden soll. In «Freiheit für alle. Das Ende der Arbeit, wie wir sie kannten» plädiert Precht deshalb für einen grundlegenden Umbau des Sozialstaates – und ein bedingungsloses Grundeinkommen.

Man darf also gespannt sein. <

# «Cybersicherheit beginnt beim Menschen»

Technische Schutzmassnahmen allein reichen heute nicht mehr aus, um Unternehmen vor Cyberangriffen zu schützen. Immer häufiger setzen Kriminelle auf psychologische Manipulation statt auf technische Schwachstellen. Wirtschaftspsychologin Jill Wick erklärt, weshalb Social Engineering so erfolgreich ist und warum Cybersicherheit zur Führungsaufgabe werden muss.

Unternehmen investieren Millionen in Firewalls und Sicherheitssysteme. Weshalb gelingt es Cyberkriminellen trotzdem immer wieder, über den Menschen zum Ziel zu kommen?

Jill Wick: Eine Antwort, die der Individualität der Menschen gerecht wird, ist in wenigen Sätzen kaum möglich. Systeme und Firewalls funktionieren nach ihrer Implementierung zuverlässig. Der Mensch ist jedoch individuell und Betrüger haben sich darauf spezialisiert, dieses Betriebssystem zu «hacken», also

Social Engineering zu betreiben. Viele unterschätzen, wie skrupellos Betrüger vorgehen, weil wir selbst ethisch denken. Das menschliche Betriebssystem hat zahlreiche Denkfehler und Schwachstellen («Biases»), die gezielt ausgenutzt werden. Darauf gehe ich auch in meinen Vorträgen ein.

**Social Engineering gehört heute zu den grössten Cyberbedrohungen. Mit welchen psychologischen Mechanismen arbeiten Angreifer besonders erfolgreich?**

Man muss zwischen geschäftlichem und privatem Kontext unterscheiden. Grundsätzlich wirken bei allen Menschen Auslöser wie Autorität («Der Chef schreibt.») oder Dringlichkeit («Ihr Konto ist gesperrt!»). Entscheidend ist jedoch, wie diese Mechanismen eingesetzt werden. Es gibt für praktisch jeden Menschen eine passende Betrugsmasche. Für die einen ist die SMS über ein angeblich nicht zugestelltes Paket gefährlich, für andere eine LinkedIn-Bekanntschaft, die plötzlich Geldanlagen empfiehlt. Ausgenutzt werden dabei unsere Denkweise, Wahrnehmung und unser Vertrauen.

Künstliche Intelligenz macht Phishing-Mails, Stimmen und sogar Videobotschaften immer glaubwürdiger. Wie verändert das die Bedrohungslage für Unternehmen?

Die grundsätzliche Bedrohungslage hat sich nicht wesentlich verändert. KI ermöglicht es Betrügern jedoch, ihre Angriffe zu verstärken und zu skalieren. Aus einem anonymen Anruf wird die Stimme der Tochter, die um Hilfe bittet, oder des CEOs, der eine sofortige Überweisung verlangt. Gleichzeitig müssen Unternehmen ihre Awareness-Programme anpassen. Schlechte Sprache oder unprofessionelle Webseiten sind heute keine verlässlichen Warnsignale mehr. KI erstellt in Sekunden überzeugende Webseiten und personalisierte Phishing-Mails. Umso wichtiger werden klare Prozesse und das Bewusstsein: Sobald jemand Geld oder Daten verlangt, sollte man besonders genau hinschauen.

**«Solange wir Betrugsopfer als dumm abstempeln, wird sich nichts ändern.»**

Viele Unternehmen führen regelmässig Security-Awareness-Schulungen durch. Woran erkennen Sie, ob eine solche Sensibilisierung tatsächlich wirkt und nicht nur eine Pflichtübung bleibt?

Von aussen ist das kaum erkennbar. Sicherheitsverantwortliche merken jedoch

Jill Wick

Wirtschaftspsychologin und Beraterin für Security Awareness

Jill Wick verbindet Psychologie, Technologie und Cybersicherheit mit besonderem Fokus auf den Menschen. Sie zeigt, wie psychologische Manipulation bei Cyberangriffen funktioniert und weshalb Security Awareness ein entscheidender Erfolgsfaktor für Unternehmen ist.



Nur die Geschäftsleitung kann Cybersicherheit dauerhaft im Unternehmen verankern. Unterstützt sie die Sicherheitsabteilung nicht, werden deren Vorgaben kaum umgesetzt. Es braucht deshalb klare Unterstützung, die nötigen personellen und finanziellen Ressourcen und eine konsequente Vorbildfunktion. Ebenso wichtig sind Ansprechpersonen im Unternehmen, die Fragen entgegennehmen, Meldungen fördern und einen konstruktiven Umgang mit Fehlern vorleben. Das schafft psychologische Sicherheit.

Welchen Aspekt rund um Security Awareness und den menschlichen Faktor möchten Sie Ihrem Publikum an der Digital Conference Ostschweiz besonders vermitteln?

Aus meiner Zeit in der Betrugsanalyse weiss ich, wie viele Menschen auf Betrug hereinfallen. Solange wir das als Dummheit abtun, wird sich nichts ändern. Verstehen wir es dagegen als menschlich, können wir besser damit umgehen. Mir ist wichtig zu vermitteln, dass es jedem passieren kann und wir Betroffene unterstützen statt verurteilen sollten. Gleichzeitig lohnt es sich, die eigenen Stärken und Schwächen zu kennen und eine höfliche Skepsis zu bewahren, besonders wenn unerwartet Geld oder Daten verlangt werden oder etwas zu gut erscheint, um wahr zu sein. <

schnell, ob Mitarbeitende aufmerksam sind. Stellen sie Fragen, melden sie verdächtige Vorfälle oder weisen sie auf Schwachstellen hin? Auch das Eingestehen eigener Fehler ist ein gutes Zeichen. Es zeigt, dass die Mitarbeitenden Verantwortung übernehmen und die Sicherheitskultur wichtiger ist als die Angst vor Konsequenzen.

Welche Verhaltensweisen oder Routinen sollten Führungskräfte vorleben, damit Cybersicherheit Teil der Unternehmenskultur wird und nicht bloss ein IT-Thema bleibt?

Führungskräfte sollten die Cybersicherheitsregeln konsequenter einhalten als alle anderen. Leider passiert oft das Gegenteil: Das C-Level verlangt Ausnahmen, etwa bei Browserfreigaben oder Sicherheitskursen. Das sendet ein falsches Signal und prägt das Verhalten der gesamten Organisation.

Was können Geschäftsleitungen tun, um Cybersicherheit dauerhaft in der Unternehmenskultur zu verankern und nicht allein der IT-Abteilung zu überlassen?

Anzeige



Universität St. Gallen

Executive School

## Cyber Security für Führungskräfte

Wie steht es um Ihre Unternehmenssicherheit?

Zertifikatslehrgang CAS der HSG –  
mögliches Startdatum: 22.-26. Februar 2027



lam.unisg.ch/csf

INFO-  
ANLÄSSE  
online

12. November 2026  
9. Dezember 2026



# «KI beschleunigt den Cyber-Wettlauf»

Quantencomputer gelten als Schlüsseltechnologie der Zukunft. Anna-Lena Horlemann, Professorin für Quantum Computing and Information Theory an der HSG, erklärt, weshalb Unternehmen die Umstellung auf quantensichere Verschlüsselung bereits heute vorbereiten sollten und wie KI die Cybersicherheit verändert.

Sie haben im Sommer 2026 an der HSG den neuen Lehrstuhl für Quantum Computing and Information Theory übernommen. Was hat Sie an diesem Forschungsgebiet so fasziniert, dass Sie ihm Ihre wissenschaftliche Laufbahn gewidmet haben?

Anna-Lena Horlemann: Quantum Computing verändert die Grundlagen der Informationsverarbeitung so grundlegend wie kaum eine Entwicklung zuvor in der Informatik. Während die klassische Informatik bis heute auf denselben Grundlagen beruht, führen Quantencomputer eine völlig neue Art des Rechnens ein. Das eröffnet nicht nur neue Anwendungsmöglichkeiten, sondern wirft auch zahlreiche wissenschaftliche Fragen auf. Gerade diese Kombination macht das Gebiet für mich besonders spannend.

Quantencomputer gelten als eine der grössten technologischen Entwicklungen der kommenden Jahre. Wo stehen wir heute tatsächlich?

Die Entwicklung hat in den vergangenen Jahren enorme Fortschritte gemacht. Die Zahl der verfügbaren Qubits ist in dieser Zeit von wenigen auf mehrere hundert gestiegen. Gleichzeitig haben sich auch die Qualität der Qubits und

die Kontrolle der Systeme deutlich verbessert. Trotzdem stehen wir erst am Anfang. Erste Konzepte und Algorithmen wurden zwar erfolgreich demonstriert; für praktisch relevante Anwendungen reicht die Rechenkapazität heutiger Quantencomputer jedoch noch nicht aus. Der entscheidende nächste Schritt besteht darin, deutlich leistungsfähigere Systeme zu entwickeln.

Ebenso wichtig ist ein realistischer Blick auf ihre Einsatzmöglichkeiten. Quantencomputer werden klassische Computer voraussichtlich nicht ersetzen, sondern sie bei ganz bestimmten Aufgaben ergänzen.

Wo sehen Sie das grösste Potenzial für praktische Anwendungen?

Zu den vielversprechendsten Einsatzgebieten gehört die Simulation von Quantensystemen, etwa für die Entwicklung neuer Materialien, chemischer Prozesse oder Medikamente. Ein weiteres wichtiges Feld sind spezielle mathematische Probleme, auf denen heutige Verschlüsselungsverfahren beruhen. Leistungsfähige Quantencomputer könnten diese künftig angreifen, weshalb bereits heute an quantensicheren kryptografischen Verfahren gearbeitet wird.

Gleichzeitig eröffnet die Quantenphysik

neue Möglichkeiten für die Cybersicherheit, etwa durch die Quantum Key Distribution, bei der die Gesetze der Quantenmechanik genutzt werden, um Manipulationsversuche beim Schlüsselaustausch unmittelbar zu erkennen. Darüber hinaus wird intensiv erforscht, ob Quantencomputer künftig auch das maschinelle Lernen bei ausgewählten Aufgaben beschleunigen können.

Sie forschen unter anderem zur Post-Quantum-Kryptographie. Weshalb sollten sich Unternehmen bereits heute mit quantensicherer Verschlüsselung befassen?

Post-Quantum-Kryptographie bezeichnet neue Verschlüsselungsverfahren, die auch Angriffen durch zukünftige leistungsfähige Quantencomputer standhalten sollen.

Der wichtigste Grund, sich bereits heute damit zu befassen, ist das sogenannte «Harvest now, decrypt later»-Szenario: Angreifer können verschlüsselte Daten bereits heute speichern und in einigen Jahren mit leistungsfähigen Quantencomputern entschlüsseln. Für Informationen, die über viele Jahre vertraulich bleiben müssen, ist das schon heute ein reales Risiko.

Viele Unternehmen fragen sich, wann sie handeln müssen. Woran erkennt ein Unternehmen, dass jetzt der richtige Zeitpunkt gekommen ist, sich mit Post-Quantum-Kryptographie auseinanderzusetzen?

Der richtige Zeitpunkt ist im Grunde jetzt. Die Migration kryptografischer Systeme kann je nach Systemlandschaft mehrere Jahre in Anspruch nehmen und



**Anna-Lena Horlemann**

**Professorin für theoretische Informatik und Mathematik, HSG**

Anna-Lena Horlemann forscht im Bereich Informationstheorie, Kodierungstheorie und Post-Quantum-Kryptographie. In ihrer Keynote zeigt sie auf, wie künstliche Intelligenz und Cybersecurity zusammenhängen und welche Entwicklungen Unternehmen künftig beschäftigen werden.

erfordert spezialisiertes Fachwissen. Gleichzeitig treiben Regulierungen in den USA, Grossbritannien und der Europäischen Union die schrittweise Umstellung bereits voran. Wer frühzeitig mit der Planung beginnt, kann die Umstellung geordnet durchführen und vermeidet später unnötigen Zeit- und Kostendruck.

**Viele Unternehmen investieren derzeit stark in künstliche Intelligenz. Wie verändert KI die Cybersicherheit?**

Künstliche Intelligenz ist ein weiteres leistungsfähiges Werkzeug im technologischen Wettlauf zwischen Angreifern und Verteidigern. Sie eröffnet neue Möglichkeiten, IT-Systeme besser zu schützen; gleichzeitig profitieren aber auch Angreifer von den rasanten Fortschritten.

KI hilft, grosse Datenmengen in Echtzeit auszuwerten, Angriffe früher zu erkennen und Sicherheitsvorfälle schneller zu analysieren. Gleichzeitig senkt sie aber auch die Hürden für Cyberangriffe. Phishing-Mails oder Social-Engineering-Angriffe lassen sich überzeugender formulieren und stärker personalisieren. Auch die Entwicklung von Schadsoftware oder die automatisierte Suche nach Schwachstellen wird erleichtert.

Der Wettlauf zwischen Angreifern und Verteidigern ist allerdings nichts Neues. KI beschleunigt diese Entwicklung zusätzlich und erhöht Tempo sowie Reichweite auf beiden Seiten.

**Wo sehen Sie bei Schweizer Unternehmen derzeit die grössten Defizite in der Cybersecurity?**

Die grösste Herausforderung ist aus meiner Sicht nicht fehlendes Problembewusstsein, sondern die Komplexität bestehender IT-Systeme. Viele Unternehmen verfügen über über Jahre gewachsene Infrastrukturen, in denen sich neue Sicherheitsanforderungen nur mit erheblichem Aufwand umsetzen lassen. Wer seine Systeme nicht gut kennt und nicht flexibel weiterentwickeln kann, wird neue Sicherheitsanforderungen nur verzögert integrieren können.

**Mit dem neuen Lehrstuhl an der HSG stärken Sie einen Forschungsbereich, der international stark an Bedeutung gewinnt. Welche Chancen ergeben sich daraus für Unternehmen in der Ostschweiz?**

Ein Lehrstuhl in diesem Bereich schafft einen direkten Zugang zu aktueller Forschung und zu hochqualifizierten Nachwuchskräften. Unternehmen erhalten

die Möglichkeit, neue Entwicklungen im Bereich Quantum Computing und Post-Quantum-Kryptographie frühzeitig kennenzulernen und mitzugestalten.

Zudem entstehen Kooperationsmöglichkeiten in Forschung und Ausbildung, etwa durch gemeinsame Projekte oder Doktorandenprogramme. Dadurch wird der Zugang zu spezialisiertem Fachwissen und zukünftigen Fachkräften unmittelbar erleichtert.

**An der Digital Conference Ostschweiz sprechen Sie zum Thema «Cybersecurity trifft KI – Risiko oder Chance?». Welche zentrale Botschaft möchten Sie Ihrem Publikum mitgeben?**

Mir ist besonders wichtig zu vermitteln, dass künstliche Intelligenz die Spielregeln der Cybersicherheit nicht neu schreibt, den technologischen Wettlauf zwischen Angreifern und Verteidigern aber deutlich beschleunigt. Sie schafft neue Angriffsmöglichkeiten, eröffnet gleichzeitig aber auch neue Werkzeuge für die Verteidigung. Gerade deshalb kommt es darauf an, die Technologie differenziert zu betrachten und ihre Chancen ebenso konsequent zu nutzen wie ihre Risiken zu adressieren.

Wer die Entwicklungen kontinuierlich verfolgt und die eigene Sicherheitsstrategie entsprechend weiterentwickelt, wird von den Chancen der KI profitieren und ihre Risiken besser beherrschen können. <

# «KI-Agenten schaffen völlig neue Angriffsflächen»

Künstliche Intelligenz verändert die Cybersecurity in rasantem Tempo. Daniel Riedener, Head Cyber Security bei der Ceruno AG und Dozent an der OST, erklärt, weshalb Unternehmen den Einsatz von KI nicht nur als Chance, sondern auch als Sicherheitsrisiko verstehen müssen, warum Prompt Injections zur realen Bedrohung werden und weshalb Angreifer derzeit noch im Vorteil sind.

Künstliche Intelligenz verändert die Cybersecurity derzeit rasanter als jede andere Technologie. Welche Entwicklung hat Sie in den vergangenen zwölf Monaten am meisten überrascht?

Daniel Riedener: Ich staune vor allem über die Geschwindigkeit, mit der sich das KI-Ökosystem entwickelt. Besonders überrascht hat mich aber, wie schnell

aus reinen Chat-Assistenten handelnde Systeme geworden sind: KI-Agenten, die selbstständig Software schreiben und ganze Aufgaben erledigen. Stichwort «Vibe Coding», bei dem Anwendungen im Dialog mit der KI entstehen. Für deren Absicherung ist bereits ein eigener Markt für Sicherheitslösungen entstanden.

Immer mehr Unternehmen setzen KI-Assistenten wie ChatGPT, Copilot oder Claude im Arbeitsalltag ein. Welche neuen Sicherheitsrisiken entstehen dadurch?

Die Risiken reichen von der Preisgabe sensibler Daten bis zur Beschädigung der eigenen Infrastruktur. Vertrauliche Informationen gelangen in KI-Modelle, Coding-Assistenten erzeugen mitunter verwundbaren Code. Mit KI-Agenten kommt eine neue Dimension hinzu: Sie versenden E-Mails, verändern Daten oder führen Befehle auf Systemen aus.

An der Digital Conference Ostschweiz sprechen Sie über «Frontier-Modelle und Prompt Injection». Was genau versteht man unter einer Prompt Injection, und weshalb sollten Unternehmen dieses Thema ernst nehmen?

Frontier-Modelle sind die jeweils leistungsfähigsten KI-Modelle ihrer Generation, etwa jene hinter ChatGPT, Claude oder Gemini. Bei einer Prompt Injection wird ein Modell über speziell formulierten Text dazu gebracht, Dinge zu tun oder preiszugeben, die es eigentlich nicht darf. Das Grundproblem: Eine KI unterscheidet im Wesentlichen nicht zwischen Daten und Instruktionen. Deshalb kann jeder verarbeitete Text versteckte Anweisungen enthalten. Ein KI-Assistent, der E-Mails zusammenfasst, könnte eine solche Anweisung als Befehl statt als Inhalt interpretieren und beispielsweise Kundenofferten an eine externe Adresse weiterleiten. Sobald Unternehmen ihre Daten mit einer KI verbinden, besteht deshalb die Gefahr,





dass genau diese KI zum Diebstahl dieser Daten missbraucht wird. Deshalb sollte jedes Unternehmen, das KI produktiv einsetzt, dieses Risiko ernst nehmen.

**Viele Unternehmen möchten KI möglichst schnell produktiv einsetzen. Wo beobachten Sie derzeit die häufigsten Fehler beim sicheren Einsatz solcher Systeme?**

Ich beobachte häufig, dass KI eingeführt wird, ohne die interne IT beziehungsweise die Security genügend einzubeziehen. Deshalb braucht es zunächst Transparenz darüber, wo im Unternehmen bereits KI im Einsatz ist, offiziell oder inoffiziell. Darauf aufbauend braucht es klare Richtlinien, freigegebene Tools als sichere Alternative und Schulungen. Das gilt besonders für KMU ohne eigenes Security-Team: Ein Verbot funktioniert erfahrungsgemäss nicht, die Mitarbeiter nutzen KI dann einfach privat und unkontrolliert weiter.

**«Angreifer können KI hemmungslos einsetzen.»**

**KI unterstützt heute nicht nur Verteidiger, sondern auch Cyberkriminelle. Wer verschafft sich derzeit den grösseren Vorteil: die Angreifer oder die Verteidiger?**

Kurzfristig sehe ich die Angreifer vorne, allerdings nicht, weil ihnen KI grundsätzlich mehr nützen würde. Beide Seiten profitieren, etwa bei der Analyse von Vorfällen oder der Erkennung von Phishing. Angreifer können KI jedoch hemmungslos einsetzen, ohne Rücksicht auf Fehler, Datenschutz oder Compliance. Für sie ist jeder Einsatz unmittelbar gewinngenerierend. Für die Verteidiger wird KI dagegen zur Doppelbelastung: Sie müssen die Technologie einerseits für die Verteidigung einsetzen und andererseits den internen Gebrauch von KI im eigenen Unternehmen absichern. Diese Asymmetrie ist aber kein Naturgesetz: Wer den eigenen KI-Einsatz früh und konsequent absichert, kann den Rückstand aufholen.

**Sie beschäftigen sich intensiv mit KI und Automatisierung in der Cybersecurity. Welche Aufgaben werden in den nächsten Jahren zunehmend von KI übernommen, und wo wird der Mensch unverzichtbar bleiben?**

In der Security ist der Wandel bereits sichtbar: Das Priorisieren von Alarmmel-

**Daniel Riedener**

**Head Cyber Security, Ceruno AG**

Daniel Riedener beschäftigt sich mit den Sicherheitsrisiken moderner KI-Systeme. Er zeigt auf, weshalb Themen wie Frontier-Modelle und Prompt Injection zunehmend an Bedeutung gewinnen und wie Unternehmen darauf reagieren können.

dungen, die Analyse grosser Datenmengen, das Erkennen von Phishing und erste Sicherheitstests übernimmt KI zunehmend schneller und in grösserem Umfang, als Menschen es je könnten. Unverzichtbar bleibt der Mensch dort, wo es um Verantwortung und weitreichende Entscheidungen geht. Wer haftet, wenn ein KI-gestütztes System einen Angriff übersieht oder in einer kritischen Situation das falsche System abschaltet? Diese Verantwortung lässt sich nicht an eine Maschine delegieren. <

Anzeige

# do-it—online

Förderangebote finden, Netzwerk entdecken, digital gründen. Im Kanton St.Gallen bist du nur ein paar Klicks von deinem Unternehmen entfernt.

do-it-in-SG.ch

Kanton St.Gallen



# «Erfolgreiche KI beginnt mit sauberen Daten»

Viele Unternehmen diskutieren über Künstliche Intelligenz, wissen aber noch nicht, wo sie sinnvoll eingesetzt werden kann. Hanspeter Pfändler von der MAIT Swiss GmbH weiss, weshalb gelungene KI-Projekte saubere Daten und klare Anwendungsfälle brauchen.



**Wo liegt der Unterschied zwischen KI-Hype und tatsächlichem Nutzen?**

Hanspeter Pfändler: Das Interesse ist zwar gross, viele wissen jedoch noch nicht, wie sie KI sinnvoll einsetzen können. Oft beschränkt sich der Einsatz auf Textverarbeitung, Recherche oder die Auswertung öffentlicher Datenmengen.

**Viele Unternehmen möchten KI rasch einsetzen. Weshalb scheitern viele Projekte früh?**

Es braucht einen klar definierten Use Case! Erst dann gibt es ein Ziel und eine Kosten-Nutzen-Abschätzung wird möglich. Fehlt diese Grundlage, wird oft einfach ausprobiert. Ebenso problematisch ist es, zuerst eine Lösung einzuführen und erst danach zu überlegen, wofür sie dienen soll.

**Ihr Vortrag heisst «Digital denken, datenbasiert handeln, mit KI skalieren».**

**Weshalb sind gute Daten so wichtig?** Erfolgreiche KI-Anwendungen basieren immer auf vorhandenen Daten. Je grösser die Datenbasis und je höher deren Qualität ist, desto sinnvoller und effizienter lässt sich KI einsetzen.

**Wo können KMU Mehrwert erzielen, ohne Millionen zu investieren?**

Viele seit Jahren genutzte Anwendungen würden heute als KI bezeichnet. Dazu gehören Ähnlichkeitssuchen zum Erkennen von Doubletten in der Produktentwicklung, die automatische Zuordnung von Rechnungen und Liefer scheinen oder die Auswertung von Maschinendaten für Vorhersagen. Wichtig ist es, bestehende Systeme konsequent zu nutzen: Daten müssen sauber gepflegt und vorhandene Funktionen richtig eingesetzt werden. Vieles ist bereits vorhanden, wird aber nicht ausgeschöpft.

**Welche organisatorischen Voraussetzungen braucht es?**

Entscheidend sind saubere, strukturierte Daten. Das gilt für die Produktentwicklung ebenso wie für die Auftragsabwicklung, von der Offerte über Produktion und Auslieferung bis zum Service. Ebenso wichtig sind klare und logische Prozesse über die gesamte Wertschöpfungskette.

**Welchen ersten Schritt empfehlen Sie?**

Unternehmen sollten prüfen, ob ihre Daten die nötige Qualität besitzen. Danach gilt es, Use Cases zu definieren und zu klären, wo KI Zeit sparen oder die Qualität verbessern kann. Darauf lässt sich eine Strategie aufbauen. Externe Unterstützung kann hier Betriebsblindheit vermeiden und Prozesse unabhängig beurteilen. <

**Hanspeter Pfändler**  
Senior Sales Manager, MAIT Swiss GmbH

Hanspeter Pfändler zeigt, wie Unternehmen Digitalisierung strategisch angehen, Daten gezielt nutzen und künstliche Intelligenz einsetzen können, um Prozesse zu optimieren und nachhaltigen Mehrwert zu schaffen.

# Weitere Speaker im Überblick

## Keynote

### 1 Henriette Engbersen

Fernsehjournalistin und  
TV-Korrespondentin

Als Leiterin des Bereichs Public Value der SRG beschäftigt sich Henriette Engbersen intensiv mit Desinformation und Medienkompetenz. Sie zeigt, weshalb Vertrauen und verlässliche Informationen im Zeitalter der künstlichen Intelligenz immer wichtiger werden.



2



## Breakout-Sessions

### 2 Sylvain Luiset

Head of Cyber Resilience  
Consulting – Switzerland, Zurich  
Insurance

Sylvain Luiset unterstützt Unternehmen dabei, Cyberrisiken verständlich zu machen und strategisch zu steuern. In seiner Breakout-Session zeigt er, weshalb Cybersecurity heute ein Business-Enabler ist und wie Unternehmen ihre Resilienz gezielt stärken können.



4



### 3 Christian Loser & Benedict Vuilleumier

Senior Consultants, Acreo Consulting ag  
Unter dem Titel «Vibe Coding trifft Compliance» zeigen Christian Loser und Benedict Vuilleumier, wie Unternehmen Innovation, Governance und regulatorische Anforderungen beim Einsatz künstlicher Intelligenz erfolgreich miteinander verbinden können.

### 4 Yannik Brühl

Incident Response Forensics Analyst,  
Arctic Wolf Networks Germany GmbH  
Yannik Brühl zeigt anhand praktischer Erfahrungen aus der Incident Response, weshalb wirksame Cybersicherheit nur gelingt, wenn Technologie, Prozesse und der Faktor Mensch zusammenspielen.

Anzeige

Sicher.  
Persönlich.  
Ceruno.



## Ist Ihre Organisation wirklich KI-ready?

Machen Sie jetzt den  
KI-Readiness-Check.

[ceruno.ch/ki-readiness-check](https://ceruno.ch/ki-readiness-check)





# Wählen Sie Ihren «Digital Shaper Ostschweiz» 2026

In den vergangenen Monaten konnten die Leser von east#digital aus über 50 Ostschweizer Persönlichkeiten und Teams ihre drei Favoriten für die Auszeichnung «Digital Shaper Ostschweiz 2026» wählen. Die zehn Personen und Teams, die bis Anfang Juli am meisten Stimmen erhalten haben, sind auf der Shortlist.

## 1 David Spoerle, Benjamin Vanzella, Lukas Naef, Lucas Roth & Michael Rey

IDIP Solution AG

Das Team der IDIP Solution AG gewann 2025 den LEADER Digital Award in der Kategorie Business. Ihre Low-Code-Plattform iDIP ermöglicht papierlose Abläufe, maschinennahe Anwendungen und digitale Prozesse ohne Programmierkenntnisse. KMU können damit Prozesse selbstständig abbilden, anpassen und erweitern, was Aufwand reduziert und Effizienz steigert. Unternehmen wie Axpo, Mövenpick oder V-ZUG setzen die Lösung bereits erfolgreich ein.

## 2 Claudio Hintermann

Co-CEO Abacus Research AG

Seit vier Jahrzehnten prägt Claudio Hintermann die Entwicklung von Abacus, das 2025 sein 40-Jahr-Jubiläum feierte und heute zu den wichtigsten Softwareanbietern der Schweiz zählt. Er trieb früh papierlose Prozesse, Automatisierung und KI voran und machte Abacus zu einem zentralen Treiber der digitalen Transformation. Mit über 65'000 Firmenkunden setzt Hintermann starke Impulse für die Ostschweizer Digitalwirtschaft.

## 3 Denis Forster

Ausbildungsverantwortlicher Informatikerberufe, Bühler AG

Mit einem praxisnahen Ausbildungskonzept gewann die Bühler AG 2025 beim

Digital Economy Award sowohl die Kategorie «ICT Education & Training» für Unternehmen mit über 100 ICT-Mitarbeitern als auch den Gesamtsieg. Das Modell verbindet digitale Lernmodule eng mit der industriellen Praxis und orientiert sich an den Lerngewohnheiten der nächsten Generation. Die Jury würdigte insbesondere den Fokus auf konkrete, im Arbeitsalltag anwendbare Kompetenzen statt auf reine Showeffekte.

## 4 Enes & Bajram Emini

Gründer Meeting Metrics

Die Brüder Enes und Bajram Emini entwickelten 2025 mit Meeting Metrics eine Plattform, die Meetings automatisch transkribiert, analysiert und zusammenfasst – auch auf Schweizerdeutsch. Das System arbeitet über drei eigene Server in St.Gallen vollständig lokal, erkennt Sprecher, erfasst Aufgaben und erstellt strukturierte Protokolle. Seit dem Start im März nutzen über 1500 Personen das Tool, das sich dank sicherer Datenverarbeitung besonders für Unternehmen eignet.

## 5 Daniel Kara & Igor Mamuzic

CEO & CIO Nägele Capaul AG

Das Traditionsunternehmen mit Wurzeln in der Funktechnik stand 2025 mit dem Projekt «NC IoT» in der Kategorie Unternehmen im Final des LEADER Digital Award. Die Plattform basiert auf der stromsparenden LoRaWAN-Technologie



und ermöglicht eine Echtzeitanalyse von Sensordaten. Dank zentralisierter Infrastruktur sinken die Betriebskosten deutlich gegenüber klassischen Systemen. Die Softwarelösung ist technisch ausgereift und für verschiedene Branchen skalierbar.

## 6 Erdin Kamoglu

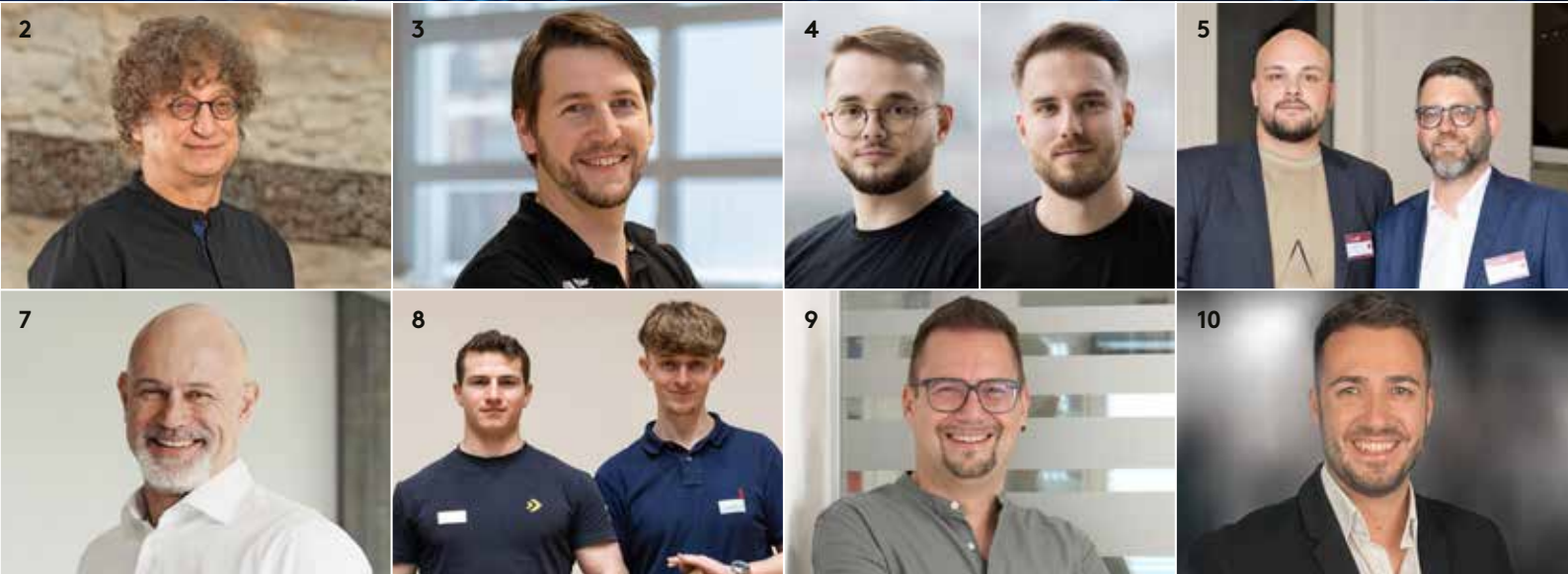
Leiter Jugendrotkreuz St.Gallen

2025 lancierte Erdin Kamoglu mit dem Jugendrotkreuz das erste «Digital Café» in St.Gallen, ein niederschwelliges Angebot, das Senioren beim Umgang mit Smartphone, Tablet oder Laptop unterstützt. Freiwillige helfen bei Fragen zu Apps, WLAN oder Online-Diensten und fördern so die digitale Teilhabe älterer Menschen. Die Initiative setzt einen wichtigen Impuls für digitale Kompetenz in der Region.

## 7 Adrian Eichrodt

CEO, Verwaltungsrat und Partner Geoinfo

2025 realisierte Geoinfo unter der Führung von Adrian Eichrodt gemeinsam



mit iNovitas eines der wichtigsten Digitalprojekte der Region: Die vollständige Erfassung aller Strassen in St.Gallen sowie in Appenzell Innerrhoden und Appenzell Ausserrhoden. Hochauflösende Kamera- und Sensorsysteme erzeugen einen digitalen Zwilling, der über Geoportal und die infra3D-Plattform präzise 3D-Daten und digitale Werkzeuge für Planung und Risikobewertungen bereitstellt.

#### 8 Kevin Willeit & Janik Meier Gründer Findmee

Kevin Willeit und Janik Meier führten Findmee 2025 zu mehreren Erfolgen: Das Start-up wurde an der Founders-Night in Chur als bestes Tech-Start-up der Südostschweiz ausgezeichnet und in das Förderprogramm von Kickstart Innovation aufgenommen. Findmee entwickelt Sensoren und Software, die Baumaschinen in Echtzeit erfassen, Laufzeiten, Auslastung und Kosten sichtbar machen und so Wartung, Diebstahlschutz und Betriebsführung digital optimieren.

#### 9 Andy Kutter

Partner & Direktor Kyos AG

Kyos entwickelte 2025 gemeinsam mit Regdata die Cybersecurity-Plattform «Kustodyan», eine Sicherheitslösung zur Daten- und API-Schutzintegration, die in diesem Jahr lanciert wurde. Die Lösung gewährleistet dynamischen Schutz durch Verschlüsselung und Tokenisierung, zugänglich über sichere APIs, kombiniert mit neu definierten, granularen Zugriffskontrollen. Kustodyan richtet sich besonders an SaaS-Hersteller aus Bereichen wie CRM, ERP, HRIS, CLM und Business-Anwendungen.

#### 10 Christian Naef

CEO und Co-Gründer RY3T

Christian Naef brachte mit RY3T eine neuartige Heiztechnologie auf den Markt: Die Serverheizung RY3T ONE nutzt die Abwärme des Bitcoin-Minings und wurde erstmals als alleinige Wärmequelle in einem Einfamilienhaus installiert. Weitere Geräte folgen in privaten Haushalten. Naef zeigt damit,

wie digitale Infrastruktur sinnvoll in die Energieversorgung integriert werden kann, und setzt einen markanten Impuls für Innovation aus der Ostschweiz.

Bis Ende August können Sie darüber abstimmen, wer von diesen zehn Personen/Teams «Digital Shaper Ostschweiz 2026» werden soll. Die Auszeichnung erfolgt im Rahmen der Digital Conference Ostschweiz 2026, die am 8. September im Einstein Congress in St.Gallen stattfinden wird.

Hier geht's zur Abstimmung >>



# Programm zur Nutzung von KI-Potenzialen in Kanton und Gemeinden

Über 120 Anwendungsfälle identifiziert.

Wo kann Künstliche Intelligenz (KI) die öffentliche Verwaltung wirksam unterstützen? Dieser Frage sind die Kantone Appenzell Ausserrhodens, Appenzell Innerrhodens, Graubünden, Thurgau, das Fürstentum Liechtenstein sowie der Kanton St.Gallen und seine Gemeinden gemeinsam nachgegangen. Dabei wurden über 120 konkrete Anwendungsfälle identifiziert – von der Büroassistenten über automatisierte Auskunftssysteme bis zur datenbasierten Entscheidungsunterstützung, gestützt auf KI-Funktionen wie Textgenerierung, Mustererkennung und Prognostik.

Die Analyse zeigt grosses Potenzial für effizientere und effektivere Behördenleistungen. Zugleich sind die Anforderungen hoch – wirtschaftlich wird der Einsatz erst, wenn Lösungen breit genutzt werden.

## Vom Potenzial zur Umsetzung: Programm bis Anfang 2027

Diese Erkenntnisse setzen der Kanton und die St.Galler Gemeinden nun um. Bis Anfang 2027 erarbeiten wir zusammen mit der Abraxas Informatik AG ein Programm, das die organisatorischen, technischen und rechtlichen Voraussetzungen für den verantwortungsvollen, sicheren und nachhaltigen Einsatz von KI in der öffentlichen Verwaltung schafft.

Im Fokus stehen der Aufbau einer kantonalen KI-Governance, die Umsetzung der Datenstrategie, die Realisierung ausgewählter Anwendungsfälle, die Etablierung eines zentralen KI-Betriebs (KI-Hub) sowie die Schaffung gezielter Schulungsangebote für Verwaltung und Gemeinden.

## Politische Absichtserklärung stärkt die Ostschweizer Zusammenarbeit

Gleichzeitig möchten wir die partnerschaftliche Zusammenarbeit auf föderaler Ebene und mit der Wirtschaft weiter stärken. Dazu haben die Kantone Appenzell Ausserrhodens, Appenzell Innerrhodens, Glarus, Graubünden, Schaffhausen, St.Gallen und Thurgau beschlossen, ihre Zusammenarbeit bei der Einführung und Nutzung von KI zu verstärken und eine politische Absichts-

erklärung unterzeichnet. Der Kanton Zürich und das Fürstentum Liechtenstein beteiligen sich als assoziierte Mitglieder der Ostschweizer Regierungskonferenz ebenfalls an der Vereinbarung.

## Synergien nutzen, Standards entwickeln, Kosten sparen

Mit der Unterzeichnung schaffen die beteiligten Kantone und das Fürstentum Liechtenstein die Grundlage, um gemeinsame KI-Projekte und Beschaffungen zu initiieren und umzusetzen. Ziel ist es, die Chancen der neuen Technologie koordiniert zu nutzen, gemeinsame Standards zu entwickeln und Doppelspurigkeiten zu vermeiden. Durch die verstärkte Zusammenarbeit können Synergien genutzt, Erfahrungen geteilt und Kosten gespart werden.

Die Analyse ist hier verfügbar:





# Cybergefahren: Ostschweizer KMU im Spannungsfeld

Die Studie «KMU Cybersicherheit 2025», an der auch die Mobiliar beteiligt ist, zeigt ein Spannungsfeld: Viele KMU treiben die Digitalisierung voran. Eine klare digitale Strategie fehlt aber bei rund einem Fünftel der befragten Firmen. Bei den übrigen sind zentrale Themen wie Datenmanagement oder künstliche Intelligenz (KI) nur teilweise umgesetzt. Gleichzeitig steigt das Risiko. Cyberangriffe sind laut Analysen der Mobiliar fünf- bis sechsmal wahrscheinlicher als ein Gebäudebrand. «Viele Ostschweizer KMU fühlen sich sicher. Sie unterschätzen aber die zunehmende Bedrohung, gerade beim Einsatz neuer digitaler Lösungen oder KI», sagt Manuel Hafner, Generalagent der Mobiliar St.Gallen. Digitalisierung und KI sind laut Hafner Chancen für Effizienz und bessere Nutzung von Daten. «Aber ohne grundlegende Cybersicherheit wird aus der Chance



schnell ein Risiko.» Die Cyberstudie zeigt, dass Updates, Firewalls und Backups verbreitet sind, organisatorische Massnahmen wie Mitarbeiterschulungen, IT-Notfallpläne oder Sicherheitsaudits aber nicht.

Hier setzt die Mobiliar mit Sensibilisierungstrainings an: Ziel ist es, Entscheidungsträger bei KMU für die strategische Bedeutung von Cyberrisiken zu gewinnen und ihre Cyber-Resilienz zu stärken.

## Die Cyberversicherung der Mobiliar – reale Hilfe im digitalen Alltag.

**Manuel Hafner**, Generalagent

**Generalagentur St. Gallen**  
Manuel Hafner  
St. Leonhard-Strasse 32, 9001 St. Gallen  
T 071 228 42 42, [stgallen@mobiliar.ch](mailto:stgallen@mobiliar.ch)  
[mobiliar.ch/stgallen](https://mobiliar.ch/stgallen)



**die Mobiliar**

223493

# St.Gallen: Ein Hotspot für KI-Innovation

Die Stadt St.Gallen zählt zu den bedeutenden ICT-Standorten der Ostschweiz und verfügt über eine starke Kompetenz im Bereich Digitalisierung und Informationstechnologie. Neben innovativen Unternehmen tragen insbesondere Bil-

dungs- und Forschungsinstitutionen wie die OST – Ostschweizer Fachhochschule und die Universität St.Gallen (HSG) dazu bei, qualifizierte Fachkräfte auszubilden und neue Technologien voranzutreiben.

Eine wichtige Rolle spielt dabei auch das Netzwerk des Vereins <IT>rockt!, das Unternehmen, Bildungsinstitutionen und Fachkräfte in der Ostschweizer ICT-Branche verbindet. Themen wie Informationssicherheit, künstliche Intelligenz, Cloud-Technologien, Softwareentwicklung und Smart-City-Konzepte gewinnen zunehmend an Bedeutung. Gleichzeitig profitieren Unternehmen von einer modernen Infrastruktur, einer guten Vernetzung sowie einem breiten Angebot an ICT-Dienstleistungen. Durch diese Kombination aus Fachwissen, Forschung, Innovation und Praxis entwickelt sich St.Gallen kontinuierlich weiter und stärkt seine Position als zukunftsorientierter ICT-Standort in der Schweiz.



## Sankt Digital



Entdecke spannende Unternehmen und Jobs in St.Gallen.

**meine-stadt.sg**

# Vertrauen ist die wichtigste Sicherheitsfunktion jeder KI

Cyber Security schützt Systeme, Netzwerke und Daten. Mit dem Einsatz von Künstlicher Intelligenz (KI) stellt sich jedoch eine weitere Frage: Wie vertrauenswürdig sind die Informationen, auf denen die KI ihre Antworten aufbaut?



Immer mehr Unternehmen setzen KI im Kundenservice, Vertrieb oder in internen Prozessen ein. Häufig unterschätzt wird dabei die Qualität der Wissensbasis. Sind Informationen veraltet, unvollständig oder widersprüchlich, entstehen Fehlentscheide und Vertrauensverlust. Denn selbst das leistungsfähigste Modell liefert nur so gute Antworten wie das Wissen, auf das es zugreift.

## Kontakt

valantic  
Fabian Ritter  
fabian.ritter@cec.valantic.com  
+41 71 313 55 70



Cyber Security endet heute nicht beim Schutz von Systemen und Daten. Ebenso wichtig ist der sichere und kontrollierte Umgang mit Unternehmenswissen. Wer Wissen strukturiert und nachvollziehbar verwaltet, schafft die Grundlage für vertrauenswürdige KI. Und Vertrauen ist nicht nur die Grundlage erfolgreicher Zusammenarbeit – es ist die wichtigste Sicherheitsfunktion jeder KI.

## Über valantic

Wir unterstützen Unternehmen dabei, digitale Kundenerlebnisse, Commerce-Plattformen und KI-Lösungen erfolgreich umzusetzen.

**valantic**

# Die grösste Schwachstelle Ihrer KI ist kein Hacker.

Breitfeldstrasse 13, 9015 St. Gallen · [valantic.com](https://valantic.com) · [info@cec.valantic.ch](mailto:info@cec.valantic.ch)



# 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.

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.

Benjamin Pipa

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



## Wir realisieren deine Vision

Willst du mit starken Videoinhalten regelmässig auf deinen Kanälen präsent sein und deine Kund:innen erreichen?

Dann wird's Zeit, dass wir uns kennenlernen.

## Bist du bereit los zu legen?



CONTENTHOUSE

Benjamin Pipa  
benjamin.pipa@contenthouse.ch  
+41 58 255 06 06

contenthouse.ch

# Cybersicherheit bei IT-Dienstleistern: Was KMU beachten sollten

Die Digitalisierung bietet KMU grosse Chancen, verlangt aber eine aktive Auseinandersetzung mit der IT-Sicherheit. Wer seine IT auslagert, delegiert zwar die Umsetzung, behält aber die Gesamtverantwortung und sollte sich gezielt mit seinem IT-Dienstleister austauschen.

## Verantwortung klären

Zunächst sollte klar sein, welche Sicherheitsbereiche der Dienstleister abdeckt und wofür das Unternehmen selbst zuständig bleibt, etwa bei eigener Software. Wichtig ist auch, wie Backups erstellt und geschützt werden: Sie sollten zuverlässig funktionieren und ausserhalb vom Firmennetzwerk oder sogar total vom Netz getrennt gespeichert sein.

## Zugriff und Überwachung absichern

Die Kundennetzwerke müssen voneinander und vom Netzwerk des Dienstleis-

ters getrennt sein. Fernzugriffe sollten durch Mehrfaktor-Authentifizierung gesichert werden. Zudem lohnt es sich, nach Überwachungssystemen, Notfallplänen und definierten Reaktionsabläufen bei Angriffen zu fragen. Offizielle Zertifizierungen bieten zusätzliche Orientierung, um die Qualität der Sicherheitsmassnahmen besser einschätzen zu können.

Suchen Sie das Gespräch mit Ihrem IT-Dienstleister und bestehen Sie auf klare Vereinbarungen. So schaffen Sie die Basis für eine sichere Zusammenarbeit. Zurich unterstützt Sie mit massgeschneiderten Cyber-Lösungen, um Ihr Unternehmen umfassend abzusichern. So bleibt Ihnen mehr Zeit, um sich auf Ihr Kerngeschäft zu konzentrieren.

Zurich, Generalagentur Alex Pfister AG  
[zurich.ch/pfister](http://zurich.ch/pfister)



**Dein KMU ist uns wichtig.  
Du bist uns wichtig.**  
Deshalb versichern wir  
deine Firma nach deinen  
Bedürfnissen.



Jetzt Termin  
vereinbaren

Zurich, Generalagentur Alex Pfister AG  
Bahnhofstrasse 27a, 9443 Widnau



# Die Zukunft der Cyberabwehr ist Teamarbeit

Cyberkriminelle nutzen KI. Unternehmen nutzen KI. Das klingt nach einem Wettrüsten. Doch wer Cybersecurity auf einen Wettbewerb der leistungsfähigsten Algorithmen reduziert, greift zu kurz. Denn Sicherheit entsteht nicht allein durch Technologie. Sie entsteht dort, wo künstliche Intelligenz und menschliche Expertise sinnvoll zusammenspielen.



Felix Guggenheim, Senior Systems Engineer bei Arctic Wolf

KI verändert die Cybersecurity grundlegend: Angreifer nutzen sie, um Phishing-Mails überzeugender zu formulieren, Schwachstellen schneller zu identifizieren und Angriffe effizienter durchzuführen. Gleichzeitig setzen Unternehmen sie ein, um Bedrohungen früher zu erkennen, grosse Datenmengen auszuwerten und Sicherheitsprozesse zu beschleunigen. Doch Geschwindigkeit allein schützt nicht. KI erkennt Muster, priorisiert Ereignisse und verarbeitet enorme Daten-

mengen in kürzester Zeit. Ob daraus tatsächlich ein Sicherheitsvorfall entsteht, welche Auswirkungen er auf das Unternehmen haben kann und welche Reaktion angemessen ist, hängt jedoch immer vom jeweiligen Kontext ab.

## Technologie braucht Erfahrung

Genau hier ergänzen sich künstliche Intelligenz und menschliche Expertise. Moderne Cybersecurity entsteht nicht durch ein Entweder-oder, sondern durch das Zusammenspiel von Technologie

und Erfahrung. Während KI dabei hilft, Millionen von Ereignissen zu analysieren und Auffälligkeiten zu priorisieren, ordnen erfahrene Security-Analysten Warnmeldungen ein, bewerten Risiken und leiten daraus konkrete Handlungsempfehlungen ab.

Erst diese Kombination sorgt dafür, dass Unternehmen ihre Aufmerksamkeit auf die Vorfälle richten können, die wirklich relevant sind.

## Das Zusammenspiel macht den Unterschied

Bei Arctic Wolf bildet dieser Ansatz die Grundlage moderner Security Operations. Künstliche Intelligenz übernimmt dort, wo Geschwindigkeit und Skalierbarkeit gefragt sind. Sicherheitsexperten ergänzen den notwendigen Kontext und unterstützen Unternehmen dabei, fundierte Entscheidungen zu treffen und wirksam auf Bedrohungen zu reagieren. Die Diskussion sollte deshalb nicht lauten, ob KI in der Cybersecurity Chance oder Risiko ist. Die eigentliche Frage ist, wie Unternehmen ihre Stärken sinnvoll mit menschlicher Expertise verbinden. Denn Cyberresilienz entsteht nicht durch Technologie allein, sondern durch ihr Zusammenspiel mit den Menschen, die sie verantwortungsvoll einsetzen.

[arcticwolf.com](https://arcticwolf.com)







# AI in cybersecurity is hard. **We make it easy.**

Partner with the world's largest agentic SOC.

[arcticwolf.com](https://arcticwolf.com)

# kustodyan<sup>®</sup>

TRUSTED DATA PROTECTION SERVICE

## WIN THE CUSTOMERS YOUR COMPETITORS CAN'T



Turn compliance into a competitive advantage.

### PROTECT



#### Sensitive customer data

Dynamic protection of sensitive customer data through encryption and tokenization

### GOVERN



#### Controlled data access

Customer-owned encryption keys and clear separation of duties ensure full control over sensitive information.

### PROVE



#### Auditable compliance

Security and compliance reporting for customers, auditors and regulators

DISCOVER HOW KUSTODYAN CAN ACCELERATE YOUR APPLICATION GROWTH

#### St. Gallen Office

Breitfeldstrasse 13

9015 St. Gallen

Tel: +41 71 566 70 30

[Kustodyan.com](https://kustodyan.com)

[kyos.ch](https://kyos.ch)

[st.gallen@kyos.ch](mailto:st.gallen@kyos.ch)

