HANDELSKAMMER
Schweiz ■ Österreich ■ Liechtenstein

Hub

Netzwerk – Wirtschaft – Trends

Das Magazin der HKSÖL

Ausgabe 2.2026

Alpenrheintal
Die exemplarische Region für wirtschaftliche Resilienz

Mehr als ein IT-Thema
Thomas Dötzl von Drei Österreich im Security-Talk

Alles sicher?
Warum Security zunehmend zur strategischen Schlüsselfrage wird

Bernina Express

Pullman Class

Stilvoll über die Alpen
St. Moritz – Tirano – St. Moritz
berninaexpress.ch/pullman-class

BERNINA EXPRESS
PULLMAN CLASS

Die Pullman Class erweitert den Bernina Express um eine eigenständige Reiseklasse

Die Fahrt in einem nostalgischen Wagen im Stil der 1930er-Jahre verbindet persönliche Betreuung, Service an Bord und Mittagessen auf einem Weingut im Veltlin zu einem sorgfältig abgestimmten Reiseprogramm. So wird die Alpenüberquerung auf der weltberühmten UNESCO-Welterbestrecke zwischen Hochgebirge und Südalpen zu einem stilvollen Rundum-Erlebnis.

Editorial

Willkommen im Hub, dem Magazin der Handelskammer Schweiz-Österreich-Liechtenstein (HKSÖL). Mit spannenden Talks und inspirierenden Storys bieten wir seitenweise News in Sachen Netzwerk, Wirtschaft und Trends.

Alexander Riklin, Präsident HKSÖL, und Urs Weber, Generalsekretär HKSÖL

Sicherheit ist längst mehr als Schutz vor Angriffen. Sie ist zur Voraussetzung für wirtschaftliche Handlungsfähigkeit geworden – in Unternehmen, Regionen und Finanzsystemen. Diese Ausgabe rückt Security deshalb als strategische Frage von Stabilität und Zukunftsfähigkeit in den Fokus.

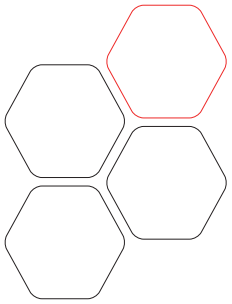
Als Presenting Partner dieser Ausgabe zeigt das Telekommunikationsunternehmen Drei Österreich, wie eng digitale Sicherheit heute mit verlässlicher Konnektivität, mobilen Arbeitsmodellen und operativer Stabilität verbunden ist. Im Interview mit Thomas Dötzl wird deutlich, warum Security für KMUs nicht bei Firewall und Virenschutz endet – sondern Geräte, Netzwerke, Zugriffe, Support und Reaktionsfähigkeit zusammengedacht werden müssen.

Auch darüber hinaus zeigt diese Ausgabe, wie breit Resilienz heute verstanden werden muss. Das Alpenrheintal steht exemplarisch für das Zusammenspiel von Infrastruktur, Industrie, Forschung und grenzüberschreitender Zusammenarbeit. Mit Teresa Loreth von Detecon sprechen wir über Business Continuity Management – und über die Frage, warum echte Krisenfestigkeit dort beginnt, wo klassische Cyberabwehr an ihre Grenzen stößt.

Ebenso beleuchten wir Cyber-Risikoanalysen, Incident Response, regulatorische Anforderungen wie das NISG 2026 und die Rechtssicherheit eines Finanzplatzes wie Liechtenstein. Denn Vertrauen entsteht dort, wo Systeme belastbar sind, Prozesse funktionieren und Risiken aktiv gemanagt werden.

Wir wünschen Ihnen viel Freude beim Lesen dieser neuen Ausgabe von Hub!

Herzlichst,
Alexander Riklin &
Urs Weber



Security ist kein Zustand, den man besitzt – sie ist eine Fähigkeit, die man ständig trainieren muss.

Inhalt

IMPRESSUM

Herausgeber, Medieninhaber:
Handelskammer Schweiz-Österreich-Liechtenstein (HKSÖL), 1040 Wien, Schwindgasse 20, hk-schweiz.at

Verleger:
MediaUnit Verlags GmbH & Co KG
Kärntner Straße 27/5. OG, 1010 Wien
office@mediaunit.at, mediaunit.at

Redaktionsleitung:
Philipp Josef Rossmann, Awedis Cocyan

Art Direction: Michaela Sattler

Chefin vom Dienst: Kristina Gut-Kisling

Projektverantwortliche HKSÖL:
Katharina Silva Guerrero

Cover: Getty Images/da-kuk, Projekt Rhesi, Thomas Dötzl (beigestellt)

Mitarbeiter dieser Ausgabe:
Brigitte Cocyan, Christine Nouikat

Anzeigen:
Awedis Cocyan
Anfragen an: a.cocyan@mediaunit.at

Druck:
Bauer Druck GmbH
Türkenstraße 8/25, A-1090 Wien
bauerdruck.com

Gedruckt auf EU-Ecolabel- und Nordic-Swan-Ecolabel-zertifiziertem Papier.

Auflage: 10.000 Stück

Aufgrund der besseren Lesbarkeit verzichten wir auf eine genderspezifische Schreibweise. Gemeint sind immer alle Lesergruppen.

Trotz präziser Recherche Angaben ohne Gewähr. Druckfehler vorbehalten.

Mehr Services unter hk-schweiz.at

Offenlegung nach Mediengesetz:
Alleiniger Medieninhaber: Handelskammer Schweiz-Österreich-Liechtenstein (HKSÖL), 1040 Wien, Schwindgasse 20, hk-schweiz.at

Grundlegende Richtung des periodischen Magazins: Es informiert zu den Themen Wirtschaft, Netzwerke und Trends. Mit Fokus auf Schweiz, Österreich, Liechtenstein. Zielgruppe sind die Keyplayer der Wirtschaft.

post.at/nachhaltig CO2 freie Zustellung 100% bis 2030

© Getty Images

Friends 4 Friends Kommunikationspartnerschaft

Nutzen Sie unsere exklusiven Friends 4 Friends Netzwerkveranstaltungen als Plattform für Ihr Unternehmen.

- **Visibility Ihrer Marke bei hochkarätigen Gästen**
- **Einladung Ihrer Zielgruppe und VIP-Kunden**
- **Medienpräsenz online & offline**

Mehr Infos und unverbindliche Anfragen:

Facetten von Raffinesse

Von dezentem Luxus über feine Kulinarik und große Klangwelten bis hin zur kraftvollen Abstraktion: vier Höhepunkte, die Sinne und Geist gleichermaßen berühren.

Text: Michaela Sattler

1

Neuer Luxus in leisen Tönen

Das „Palais Coburg" richtet sich neu aus: Das traditionsreiche Haus im Herzen Wiens wird derzeit umfassend renoviert und soll im Sommer 2026 als exklusives Private Guesthouse mit 36 individuell gestalteten Suiten wiedereröffnen. Der Fokus liegt dabei auf Privatsphäre, Personalisierung und Quiet Luxury. Dabei bleibt die historische Substanz erhalten und wird behutsam in die Gegenwart übersetzt. Charakteristische Räume wie die Bel Étage, die Kasematten und das renommierte Weinarchiv bleiben zentrale Bestandteile des Hauses. Kulinarisch setzt das Palais bereits während der Renovierung Akzente: Das mit zwei Michelin-Sternen ausgezeichnete Restaurant „Silvio Nickol" sowie die „Clementine im Glashaus" bleiben geöffnet. **palais-coburg.com**

2
Neuer Glanz in Zürich

Mit der „Villa Florhof“ gewinnt Zürich im Juni 2026 ein stilvolles Refugium, das historische Substanz mit zeitgemäßem Design verbindet. Das denkmalgeschützte Patrizierhaus wurde behutsam revitalisiert und als Boutiquehotel neu interpretiert. Herzstück ist das Fine-Dining-Restaurant, das von Christian Jürgens geleitet wird. Er ist bekannt für seine präzise, kreative Haute Cuisine. Das Haus bietet 13 individuell gestaltete Zimmer und Suiten, eine elegante Bar, eine stilvolle Lounge, einen exklusiven Fumoir und den historischen Gewölbekeller. Unter der Gesamtleitung von Tanja Wegmann (General Manager Lalique Hospitality) und Christian Jürgens entsteht ein Ort, der Design, Kultur und Kulinarik auf höchstem Niveau vereint. **villaflorhof.com**

3
Sommerklang in Luzern

Vom 13. August bis 13. September 2026 findet das Lucerne Festival unter der Leitung von Intendant Sebastian Nordmann statt. Unter dem Motto „American Dreams“ stehen Werke von George Gershwin, Charles Ives, Aaron Copland oder Samuel Barber im Zentrum, präsentiert von internationalen Spitzenorchestern und Solisten wie Yuja Wang, Augustin Hadelich oder Anne-Sophie Mutter, die ihr 50-jähriges Bühnenjubiläum feiert. Neu im Programm sind immersive Konzertformate wie Mittendrin, das Open-Air-Event Klassik für alle und das Straßenmusik-Festival City Stage, das sechs Tage lang überraschende Pop-up-Konzerte quer durch Luzern bietet. **lucernefestival.ch**

4
Die Kraft der Abstraktion

Die Ausstellung „Abstrakt“ lädt bis zum 17. Mai 2027 in der Hilti Art Foundation dazu ein, die Faszination der Abstraktion zu entdecken. Zu Beginn des 20. Jahrhunderts entwickelten Künstler eine Bildsprache, die nicht mehr das Sichtbare abbilden, sondern radikal modern und weltweit verständlich sein sollte. Wissenschaft, Technik und die Suche nach dem Geistig-Seelischen trieben diese Kunst an, die sich ganz auf Linien, Farben und Formen reduzierte. Im Zentrum der Ausstellung stehen rund 60 Werke, darunter drei bedeutende Neuerwerbungen von Carmen Herrera, Wassily Kandinsky und Mark Rothko. Umgeben von weiteren Gemälden und Skulpturen der Sammlung zeigen sie drei unterschiedliche Spielarten der Abstraktion: das Loslösen vom Gegenstand, die geometrische Konstruktion und die Farbfeldmalerei. Kuratiert wurde die Ausstellung von Karin Schick, Direktorin der Hilti Art Foundation. **haf.li**

Das Alpenrheintal

In einer der dynamischsten Industrieregionen des Alpenraums wird Sicherheit neu definiert – nicht als Einzelmaßnahme, sondern als integriertes System, das physische Stabilität, technologische Präzision und wirtschaftliche Stärke verbindet.

Text: Brigitte Cocyan

Das Alpenrheintal verbindet Österreich, die Schweiz und Liechtenstein zu einem eng verflochtenen Wirtschafts- und Lebensraum zwischen Bodensee und Alpen.

Zwischen Bodensee und Alpen ist ein Wirtschaftsraum entstanden, der nationale Grenzen im Alltag längst überschreitet. Vorarlberg, das St. Galler Rheintal und das Fürstentum Liechtenstein bilden ein eng vernetztes Industrie- und Technologiedreieck. Die Region gilt als eine der exportstarken und innovationsgetriebenen Zonen im Alpenraum – mit einer außergewöhnlich hohen Dichte an Industrieunternehmen, spezialisierten Zuliefernetzwerken und anwendungsnaher Forschung.

Gerade aus der Perspektive von Security ist das Alpenrheintal bemerkenswert, weil sich hier ein erweitertes Verständnis von Resilienz beobachten lässt. Sicherheit ist in diesem Kontext weder ausschließlich eine Frage von Cyberabwehr noch von physischem Schutz. Sie entsteht vielmehr aus dem Zusammenspiel mehrerer Ebenen, die ineinandergreifen und sich gegenseitig stabilisieren – physisch, technologisch und wirtschaftlich.

Sicherheit beginnt im Flussbett

Den Ausgangspunkt bildet die physische Resilienz des Lebensraums selbst. Der Alpenrhein ist seit jeher prägend für die Region – als Verkehrsachse, Energiequelle und zugleich als latente Bedrohung. Mit dem Projekt „Rhesi“ (Rhein, Erholung und Sicherheit) setzen Österreich und die Schweiz eines der größten Hochwasserschutzvorhaben Europas um. Das Projekt steht exemplarisch für einen Paradigmenwechsel im Umgang mit Naturgefahren: Statt den Fluss ausschließlich durch technische Barrieren zu kontrollieren, wird ihm durch gezielte Aufweitungen wieder mehr Raum gegeben. Ziel ist ein Schutz gegen Extremereignisse, die statistisch etwa alle 300 Jahre auftreten können.

Diese Form der Risikosteuerung hat unmittelbare Auswirkungen auf die wirtschaftliche Stabilität der Region. Industrieanlagen, Verkehrswege und Siedlungsräume werden nicht nur geschützt, sondern langfristig kalkulierbar gemacht. Für exportorientierte Unternehmen, deren Wertschöpfung stark von stabilen Produktions- und Lieferketten abhängt, ist diese Planbarkeit ein zentraler Standortfaktor. Physische Sicherheit wird damit zur stillen Voraussetzung für alles Weitere – auch für digitale und organisatorische Sicherheitskonzepte.

Projekt „Rhesi“: grenzüberschreitendes Hochwasserschutzprojekt am Alpenrhein für mehr Sicherheit von Region, Infrastruktur und Industrie.

Das Nervensystem der Industrie

Auf dieser Grundlage entwickelt sich im Alpenrheintal eine zweite Ebene der Resilienz, die zunehmend an Bedeutung gewinnt: die technologische Sicherheit. Am Campus Buchs entsteht mit dem Sensor Innovation Hub ein Knotenpunkt, an dem Forschung und Industrie eng zusammenarbeiten. Im Zentrum steht die Entwicklung und Anwendung hochpräziser Sensorsysteme, die in modernen Industrieumgebungen eine Schlüsselrolle einnehmen.

Sensorik fungiert gewissermaßen als „Nervensystem“ vernetzter Infrastrukturen. Sie ermöglicht die kontinuierliche Überwachung von Produktionsanlagen, liefert Zustandsdaten von Brücken, Energieversorgungssystemen oder industriellen Prozessen und bildet die Grundlage für Frühwarnmechanismen. Gerade im Kontext von Industrial IoT und vernetzter Fertigung wird deutlich, dass in puncto Sicherheit nicht mehr klar zwischen physischer und digitaler Ebene getrennt werden kann. Ein manipuliertes Sensorsignal, eine fehlerhafte Messkette oder ein Ausfall in der Datenübertragung kann unmittelbare reale Konsequenzen nach sich ziehen – von Produktionsstillständen bis hin zu sicherheitskritischen Fehlentscheidungen. Die Fähigkeit, solche Risiken frühzeitig zu erkennen und zu kontrollieren, wird damit zu einem zentralen Bestandteil moderner Sicherheitsarchitekturen. Präzision, Robustheit und Integrität von Messdaten sind nicht nur technische Qualitätsmerkmale, sondern entscheidende Faktoren für die Resilienz industrieller Systeme.

Schutzfaktor Know-how

Diese technologische Dimension trifft im Alpenrheintal auf eine wirtschaftliche Struktur, die stark von Spezialisierung und globaler Vernetzung geprägt ist. Unternehmen wie Hilti, Blum, Zumtobel Group oder Leica Geosystems stehen exemplarisch für eine Industrie, deren Wettbewerbsfähigkeit maßgeblich auf Know-how, Prozessqualität und technologischer Differenzierung beruht.

Damit rückt eine dritte Ebene der Resilienz in den Fokus: die wirtschaftliche und digitale Sicherheit. Der Schutz von geistigem Eigentum, von Entwicklungsdaten und von sensiblen Produktionsprozessen wird zunehmend geschäftskritisch. Gleichzeitig steigen mit der Vernetzung von Produktionssystemen die Angriffsflächen für Cyber-

Industrial IoT: Überwachung vernetzter Produktions- und Sensorsysteme in Echtzeit – an der Schnittstelle zwischen Daten, Infrastruktur und industrieller Sicherheit.

bedrohungen. Sicherheitsfragen verlagern sich dadurch immer stärker in die operative Ebene der Industrie – dorthin, wo Italien und Osttirol zusammenwachsen. Im Alpenrheintal zeigt sich, wie dieser Herausforderung begegnet werden kann. Initiativen wie der Switzerland Innovation Park Ost schaffen Strukturen, in denen Forschung und Industrie gemeinsam an Lösungen arbeiten. Der Fokus liegt dabei nicht nur auf technologischer Innovation, sondern auch auf deren sicherer Integration in bestehende Systeme. Es entsteht ein Umfeld, in dem neue Technologien unter realistischen Bedingungen entwickelt, getestet und implementiert werden können – inklusive der dazugehörigen Sicherheitsanforderungen.

Ein System, kein Einzelprojekt

Auffällig ist dabei, wie eng die verschiedenen Ebenen der Resilienz miteinander verknüpft sind. Der Hochwasserschutz sichert die physische Grundlage industrieller Tätigkeit. Die Sensorik liefert die Daten, um Systeme zu überwachen und Risiken frühzeitig zu erkennen. Und die wirtschaftliche sowie digitale Sicherheit sorgen dafür, dass Innovationen und Wertschöpfung langfristig geschützt werden können. Keine dieser Ebenen funktioniert isoliert – erst im Zusammenspiel entsteht ein belastbares Gesamtsystem.

Das Alpenrheintal ist damit weniger ein spektakuläres „Epizentrum" als vielmehr ein präzise austariertes Modell für moderne Resilienz. Die Besonderheit liegt nicht in einzelnen Leuchtturmprojekten, sondern in der konsequenten Verzahnung von Infrastruktur, Technologie und Wirtschaft über nationale Grenzen hinweg. Die Zusammenarbeit zwischen Österreich, der Schweiz und Liechtenstein ist dabei keine abstrakte politische Idee, sondern gelebte Praxis im industriellen Alltag.

Für Unternehmen im Security-Umfeld ergibt sich daraus ein klarer Erkenntniswert: Resilienz entsteht dort, wo physische, technologische und wirtschaftliche Sicherheitsaspekte gemeinsam gedacht und umgesetzt werden. Das Alpenrheintal liefert dafür ein konkretes, übertragbares Beispiel – nicht als theoretisches Konzept, sondern als funktionierendes System unter realen Bedingungen.

SHORT FACTS

Drei Länder, ein System
Österreich (Vorarlberg), Schweiz (St. Galler Rheintal) und Liechtenstein agieren als eng verflochtener Wirtschaftsraum.

Hohe Exportquote
In Vorarlberg und Liechtenstein liegt sie deutlich über dem EU-Schnitt (teils über 70 %).

Industrie als Rückgrat
Rund ein Drittel der Wertschöpfung entfällt in Vorarlberg auf die Industrie – deutlich über dem europäischen Durchschnitt.

Liechtenstein: global vernetzt
Einer der weltweit höchsten Industrialisierungsgrade pro Kopf, stark exportorientiert.

Unternehmensdichte
Hohe Konzentration international tätiger Mittelständler und Weltmarktführer auf engem Raum.

Projekt Rhesi
Hochwasserschutz für ein Einzugsgebiet mit rund 300.000 Menschen; Auslegung auf Extremereignisse im 300-Jahres-Rhythmus.

Forschung & Innovation
Institutionen wie der Sensor Innovation Hub in Buchs stärken den direkten Wissenstransfer in die Industrie.

Industrial IoT
Hoher Digitalisierungsgrad in der Produktion – mit entsprechend steigenden Anforderungen an Cyber-Security.

Mehr zur Region:

10 Jahre Grand Train Tour of Switzerland

Die schönste Zugreise durch die Alpen

Die Schweiz zieht Reisende und Entdeckungsfreudige seit Jahrhunderten an. Seit nunmehr einem Jahrzehnt verbindet die Grand Train Tour of Switzerland die bekanntesten Panoramastrecken des Landes. Sie vereint Natur und Kultur – komfortabel, nachhaltig und ganz ohne Auto. Hier entdeckt man die Schweiz aus einigen ihrer eindrucksvollsten Perspektiven.

Eine Reise voller Höhepunkte
Auf insgesamt 1.280 Kilometern führt die Route entlang klarer Seen, über alpine Pässe und durch UNESCO-Welterbestätten. Großzügige Panoramafenster eröffnen weite Blicke auf wechselnde Landschaftsformen – vom mediterran geprägten Tessin bis zur hochalpinen Region Graubündens.

Die beste Zeit für eine Bahnentdeckung
Die Grand Train Tour of Switzerland lässt sich ganzjährig bereisen. Von den kühlen, klaren Wintertagen bis zu den langen Abenden im Sommer zeigen sich die Jahreszeiten in Licht, Farben und Atmosphäre. Besonders komfortabel wird die Reise mit dem Swiss Travel Pass, der freie Fahrt auf Bahn, Bus und Schiff ermöglicht – inklusive Premium-Panoramazügen und zahlreichen Museumseintritten.

Fünf Premiumlinien, ein vielseitiges Erlebnis
Zum Jubiläum stehen die fünf Premiumlinien der Tour im Mittelpunkt: Glacier Express zwischen Zermatt und St. Moritz, Bernina Express über das UNESCO-Welterbe ins südliche Tessin, Gotthard Panorama Express als Schiff-Zug-Kombination, GoldenPass Express vom Genfersee nach Interlaken sowie der Luzern–Interlaken Express durch die Zentralschweiz.

Flexibel und einfach erreichbar
Das Schweizer öffentliche Verkehrsnetz ist das dichteste der Welt. Perfekt abgestimmte Fahrpläne reduzieren Wartezeiten und erleichtern einen entspannten Reiseablauf. So erlebt man jene Qualitäten, die die Schweiz seit Generationen zu einem beliebten Reiseziel machen.

Highlights

- Gesamtlänge: 1.280 km
- Etappen: 8
- UNESCO-Welterbestätten: 5
- Saison: ganzjährig
- Ticketempfehlung: Der Swiss Travel Pass bietet internationalen Gästen freie Fahrt in der ganzen Schweiz.
- Anreise: Für Gäste aus Österreich gibt es bis zu sechs tägliche Direktverbindungen zwischen Wien und Zürich.

Weitere Informationen:

switzerland.com/gttos

Überlebensfrage Security

Warum Resilienz in einer vernetzten Welt zur neuen harten Währung und zur Grundlage unternehmerischer Handlungsfähigkeit wird.

Text: Brigitte Cocyan

Früher war Sicherheit im Wirtschaftsleben ein Zustand, den man durch das Abschließen von Türen und das Installieren von Firewalls erreichte. Es war eine statische Barriere gegen die Außenwelt, ein mechanischer Schutzwall, der eine klare Grenze zwischen dem Innen und dem Außen zog. Im Jahr 2026 hat sich dieses Bild radikal gewandelt. In einer hypervernetzten Welt, in der die Grenzen zwischen physischer Infrastruktur, digitalem Datenaustausch und globalen Lieferketten verschwimmen, ist Sicherheit kein Zustand mehr, den man besitzt – sie ist eine Fähigkeit, die man ständig trainieren muss. Wir befinden uns in der Ära der organisationalen Resilienz. Wer im digitalen Sturm der kommenden Jahre bestehen will, darf Sicherheit nicht länger als lästige Kostenstelle begreifen, sondern als das fundamentale Betriebssystem, auf dem jede Form von Innovation und Wachstum erst möglich wird. In einer Welt, in der das Wegsehen zum größten Risiko geworden ist, markiert das neue Bewusstsein den Übergang von der rein technischen Abwehr hin zu einer strategischen Überlebensfrage.

Das Ende der Naivität und der juristische Wendepunkt

Lange Zeit galt das Thema Sicherheit in vielen Chefetagen als notwendiges Übel – als Aufgabe, die tief im Keller der IT-Abteilung vergraben war. Doch das Jahr 2026 markiert einen historischen Wendepunkt für die Unternehmensführung. Mit dem Inkrafttreten des NISG 2026 am 1. Oktober ist Cybersicherheit endgültig im Sitzungssaal angekommen. Das Gesetz weitet den Kreis der betroffenen Unternehmen massiv aus und unterwirft tausende Betriebe strengen Meldepflichten sowie verpflichtenden Sicherheitsvorgaben. Die Tragweite reicht jedoch weit über die unmittelbar regulierten Branchen hinaus, da das Gesetz explizit die Sicherheit der gesamten Lieferkette fordert. In der Praxis bedeutet dies, dass jeder Zulieferer oder Dienstleister eines betroffenen Unternehmens über kurz oder lang vertraglich dazu verpflichtet wird, die gleichen hohen Sicherheitsstandards ein-

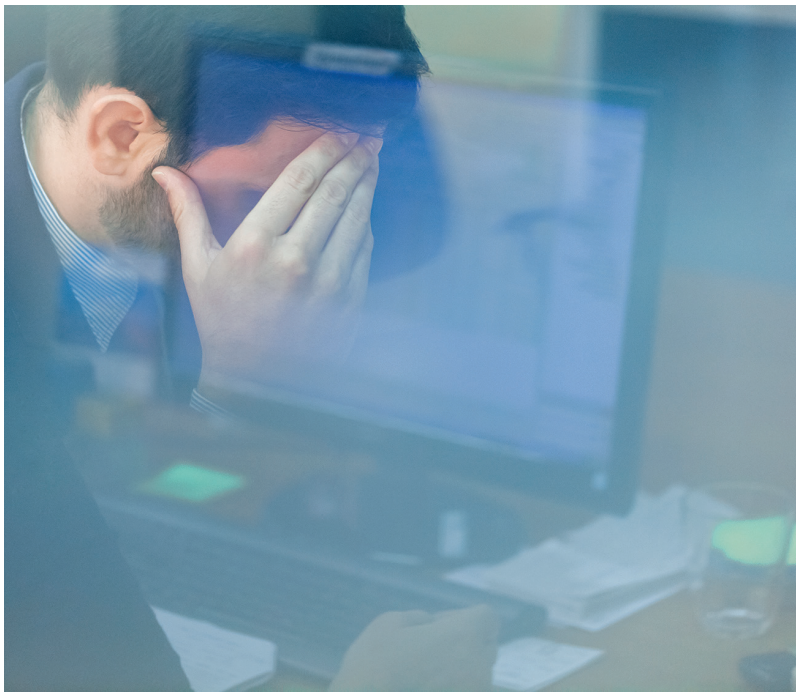
In einer Welt aus Datenströmen und Abhängigkeiten wird Resilienz zur tragenden Struktur unternehmerischer Stabilität.

zuhalten. Damit wird Cybersicherheit zu einer neuen Form der Kreditwürdigkeit im B2B-Sektor. Wer heute als Geschäftsführer die Verantwortung an die IT delegiert, ohne sie strategisch zu führen, riskiert im Ernstfall nicht nur Bußgelder in Millionenhöhe, sondern auch seine persönliche Haftung und die faktische Marktfähigkeit des Unternehmens. Die Gesetzgebung spiegelt damit eine neue Realität wider, in der ein Ausfall kein privates Pech mehr darstellt, sondern ein systemisches Risiko für das gesamte ökosystemische Umfeld. Die wahre Bedrohung ist dabei jedoch nicht die Behörde, sondern die drastisch verkürzte Reaktionszeit der Angreifer. Während Hacker früher Monate im Netzwerk verbrachten, dauert es heute oft nur noch wenige Wochen vom ersten Zugriff bis zur kompletten Verschlüsselung. In einer Welt, in der die Mehrheit der Unternehmen bereits Opfer von Angriffen wurde, verschiebt sich der Fokus: Die Frage ist nicht mehr, ob ein Einschlag erfolgt, sondern wie belastbar das Unternehmen darauf reagiert.

Das Sicherheitsnetz als strategische Überlebensversicherung

In der Krise ist Liquidität alles. Was die Frage aufwirft, ob man Risiken schlichtweg wegversichern kann. Die Antwort im Jahr 2026 ist differenziert, denn Versicherer agieren heute als strenge Hüter der Standards. Wer seine Hausaufgaben in der Prävention nicht gemacht hat, erhält keinen Schutz oder bleibt im Schadensfall auf den Kosten sitzen. Ein modernes Risikomanagement ruht dabei auf Säulen, die weit über rein finanzielle Entschädigungen hinausgehen. Die Cyber-Polizze beinhaltet heute als eine Art digitales Sondereinsatzkommando, das im Schadensfall nicht nur den technischen Wiederaufbau finanziert, sondern vor allem IT-Forensiker, spezialisierte Rechtsanwälte und Krisenkommunikatoren bereitstellt, um den Reputationsschaden zu begrenzen.

Flankiert wird dies durch Konzepte wie Kidnap & Ransom, die in einer global agierenden Wirtschaft längst nicht mehr nur klassische Entführungen abdecken, sondern massiv digitale Erpressungsszenarien mit sensiblen Kundendaten adressieren. Der entscheidende Wert liegt hier im sofortigen Zugang zu professionellen Verhandlungsführern, die in Extremsituationen kühlen Kopf bewahren. Darüber hinaus bedeutet Resilienz auch, die menschliche Kontinuität zu hinterfragen und die Absicherung von Schlüsselpersonen mitzudenken. Es gilt zu klären, was passiert, wenn



Der Moment der Störung bleibt oft unsichtbar – bis sich zeigt, wie verletzlich vernetzte Systeme im Ernstfall tatsächlich sind.

nicht der Server, sondern der Kopf des Unternehmens durch Krankheit, Unfall oder politische Krisen ausfällt. Versicherungen mildern zwar den finanziellen Schmerz, aber sie reparieren keine verlorenen Kundenbeziehungen oder unterbrochenen Lieferketten.

Die Fronten der Resilienz: Infrastruktur, Krise und Mensch

Echte Resilienz entsteht dort, wo das Management proaktiv die eigenen blinden Flecken identifiziert. Oft scheitern Unternehmen daran, dass sie ihre Verwundbarkeit gegenüber Dritten und externen Abhängigkeiten wie Cloud-Plattformen oder Logistikdienstleistern unterschätzen. Dabei muss die Widerstandsfähigkeit an verschiedenen Fronten gleichzeitig aufgebaut werden. An der technologischen Front muss Sicherheit bereits im Netzwerk ansetzen, um Bedrohungen abzufangen, bevor sie die Endgeräte erreichen. In einer Zeit mobiler Arbeit und standortübergreifender Vernetzung ist die klassische Burgmauer-Sicherheit ums Büro längst obsolet geworden.

Ebenso wichtig ist die operative Ebene: Ein Business Continuity Management darf kein Dokument für die Schublade sein, sondern muss als lebender Prozess verstanden werden. Es verlangt nach Krisenplänen, die in realitätsnahen Simulationen erprobt wurden, denn nur wer den Ernstfall übt, behält im Chaos die Kontrolle. Schließlich bleibt die menschliche Front entscheidend. Trotz aller technologischen Aufrüstung ist der Faktor Mensch oft das primäre Ziel von Manipulationen durch Phishing oder Social Engineering. Eine resiliente Organisation zeichnet sich dadurch aus, dass sie Sicherheit nicht als starres Verbotssystem, sondern als gelebte Unternehmenskultur begreift. Mitarbeitende müssen zu einem sensorischen Frühwarnsystem werden, das Anomalien erkennt und meldet, bevor sie sich zum Flächenbrand ausweiten. Sicherheit im Jahr 2026 ist kein notwendiges Übel, sondern das Vertrauensversprechen, dass ein Unternehmen ein verlässlicher Teil der globalen Wertschöpfungskette bleibt. Es ist die Basis für Stabilität und führt zu einer professionellen Außenwirkung, die in einer unvorhersehbaren Welt zur wichtigsten Investition des Jahrzehnts wird.

RESILIENZ IST DIE NEUE WÄHRUNG

Fünf Faktoren, die über Stabilität, Vertrauen und Marktfähigkeit entscheiden:

- **Chefsache, nicht IT-Thema**
  Cybersicherheit ist strategische Führungsverantwortung. Mit der NIS-2-Richtlinie haften Geschäftsführer persönlich für Sicherheitsversäumnisse. Wer Risiken versteht, Budgets freigibt und Notfallpläne steuert, macht Cyberresilienz zur Unternehmensaufgabe – nicht zur IT-Pflicht.

- **Die Lieferkette ist Teil des Risikos**
  Angriffe passieren oft über Dritte. Partner, Zulieferer und Cloud-Anbieter sind Teil der eigenen Sicherheitsarchitektur. Transparente Standards, Audits und klare Verträge schützen vor Folgeschäden – besonders in vernetzten Produktionsumgebungen.

- **Reaktion schlägt Illusion von Kontrolle**
  Perfekter Schutz ist illusorisch. Entscheidend ist die Fähigkeit, schnell und professionell auf Angriffe zu reagieren. Klare Incident-Response-Pläne, getestete Kommunikationswege und forensische Unterstützung entscheiden über Schaden oder Stabilität.

- **Schutz als Service**
  Moderne Cyber-Polizzen sind mehr als Schadensersatz: Sie sichern Zugang zu Experten für Forensik, Recht und Krisenkommunikation. So wird im Ernstfall aus Versicherung echte Widerstandskraft – ein integraler Bestandteil der Business-Continuity-Strategie.

- **Der Mensch ist das System**
  Technik ist nur so stark wie ihre Anwender. Eine aktive Sicherheitskultur mit Schulungen, offenen Meldewegen und geübtem Verhalten reduziert Risiken signifikant. Resilienz entsteht, wenn Mitarbeitende verstehen, wie sie Teil der Verteidigung sein können.

Cybersicherheit 2026 – die Details zum NISG:

Mehr als IT-Schutz

Wie sich Cyber-Security heute ganzheitlich denken lässt, wo die größten Risiken liegen und welche pragmatischen Lösungen insbesondere für KMUs relevant sind, erklärt Thomas Dötzl, Head of 3rd Party Retail bei Drei Österreich.

Text: Philipp Josef Rossmann

Kaum ein Thema hat sich in den vergangenen Jahren so stark weiterentwickelt wie digitale Sicherheit. Längst geht es nicht mehr nur um den Schutz einzelner Systeme, sondern um die Resilienz gesamter Geschäftsmodelle. Vernetzte Arbeitswelten, mobile Endgeräte und cloudbasierte Prozesse erweitern nicht nur die Möglichkeiten für Unternehmen, sondern auch deren Angriffsflächen. Gerade kleine und mittlere Betriebe stehen dabei vor einem Spannungsfeld: steigende Anforderungen bei gleichzeitig begrenzten Ressourcen. Security muss heute mit dem Alltag Schritt halten — unkompliziert, verlässlich und integrativ gedacht. Wie Unternehmen diesen Wandel bewältigen können, erklärt Thomas Dötzl, Head of 3rd Party Retail bei Drei Österreich, im Gespräch.

Sicherheit ist für Unternehmen längst mehr als ein IT-Thema. Wie hat sich der Begriff Security aus Ihrer Sicht in den vergangenen Jahren verändert?

Früher war Security stark von klassischen IT-Schutzmaßnahmen geprägt, etwa Firewall, Virenschutz und Gerätesicherheit. Heute ist das deutlich breiter. Security betrifft nicht mehr nur die IT, sondern den gesamten Geschäftsbetrieb: Erreichbarkeit, Datenverfügbarkeit, mobile Arbeit, sichere Kommunikation und Zugriff auf Unternehmensressourcen. Für uns ist Security deshalb heute kein isoliertes Technikthema mehr, sondern ein zentraler Bestandteil eines stabilen und reibungslosen Geschäftsbetriebs. Es geht darum, dass Unternehmen im Alltag zuverlässig arbeiten können. Auch dann, wenn etwas Unvorhergesehenes passiert.

Viele KMUs verbinden Security noch immer vor allem mit Antivirus-Software und Firewalls. Wo beginnt digitale Sicherheit heute tatsächlich — und wie umfassend muss man das Thema inzwischen denken?

Digitale Sicherheit beginnt heute viel früher: bei der Frage, welche Geräte im Einsatz sind, wie sie verwaltet werden, wer worauf zugreifen darf, wie Standorte vernetzt sind und wie schnell ein Unternehmen im Ernstfall reagieren kann. Antivirus und Firewall sind nur einzelne Elemente. Heute muss man Security ganzheitlich betrachten: als netzbasierten Schutz, Geräteschutz, Update-Management, sichere mobile Nutzung, klare Berechtigungen, Absicherung verteilter Arbeitsplätze und laufende Betreuung. Genau in diese Richtung argumentieren auch wir mit Lösungen wie Internetschutz Pro, Mobile Device Management und sicheren Vernetzungsstrategien.

Unternehmen investieren viel in Effizienz, Wachstum und Digitalisierung. Warum wird Security in der Praxis trotzdem oft erst dann priorisiert, wenn bereits ein Vorfall passiert ist?

Weil Security für viele Unternehmen noch immer primär als Kostenblock wahrgenommen wird und ihr Nutzen dann am sichtbarsten wird, wenn etwas schiefgeht. Effizienz- oder Wachstumsinvestitionen wirken unmittelbar positiv, Sicherheitsinvestitionen oft eher präventiv und damit weniger greifbar. Dazu kommt: Gerade KMUs haben wenig Zeit und oft keine eigene Security-Spezialisierung. Dann rutschen Themen wie Richtlinien, Geräteverwaltung oder Notfallreaktion im Alltag nach hinten. Dass das riskant ist, zeigen auch Zahlen aus einer Drei-Presseaussendung: 45 Prozent der Unternehmen schätzen die Gefahren von Cyberkriminalität als gering ein, während es bei 47 Prozent bereits zu Vorfällen gekommen ist.

Wo sehen Sie aktuell die größten Sicherheitsrisiken für KMUs: bei der technischen Infrastruktur, bei mobilen Endgeräten, im Faktor Mensch oder in unklaren Prozessen?

Thomas Dötzl,
Head of 3rd Party Retail, Drei Österreich

Am größten ist meist nicht ein einzelner Punkt, sondern die Kombination daraus. Wenn ich priorisieren müsste, würde ich sagen: erstens der Faktor Mensch, etwa bei Phishing und Social Engineering; zweitens mobile Endgeräte, weil sie heute zentrale Arbeitswerkzeuge sind und oft außerhalb klassischer Firmen-IT genutzt werden; drittens unklare Prozesse, etwa fehlende Zuständigkeiten bei Verlust, Berechtigungen oder Updates. Auch die Drei-Unternehmensumfrage nennt Phishing/Social Engineering und Malware als häufige Vorfälle. Und aus unserer Sicht werden Risiken vor allem dann groß, wenn Geräte, Netz, Nutzerverhalten und Prozesse nicht zusammengedacht werden.

Gerade kleinere und mittlere Unternehmen haben oft keine eigene große IT- oder Security-Abteilung. Wie lässt sich ein belastbares Sicherheitsniveau erreichen, ohne dass Komplexität und Kosten sofort zum Ausschlusskriterium werden?

Der entscheidende Punkt ist: Security muss für KMUs einfach, skalierbar und betreibbar sein. Nicht alles selbst bauen, sondern pragmatisch mit integrierten Lösungen arbeiten. Ein belastbares Grundniveau entsteht oft schon durch wenige, sauber umgesetzte Maßnahmen: sichere Konnektivität, Schutz vor schädlichen Seiten und Malware, zentrale Verwaltung mobiler Geräte, klare Regeln für Zugriffe und ein verlässlicher Supportfall, wenn etwas passiert. Genau das ist für KMUs wichtig: nicht maximale Komplexität, sondern ein sinnvoller Sicherheitsstandard, der im Alltag tatsächlich gelebt werden kann. Drei positioniert hier Lösungen, die eher vereinfachen als verkomplizieren – etwa Internetschutz Pro (oder Miradore MDM).

Mit zunehmender Mobilität, Cloud-Nutzung und standortübergreifender Zusammenarbeit wächst auch die Angriffsfläche. Welche Fehler beobachten Sie bei Unternehmen besonders häufig, wenn digitale Arbeitsmodelle eingeführt werden?

Ein häufiger Fehler ist, neue Arbeitsmodelle schnell einzuführen, ohne die Sicherheitslogik mitzudenken. Dann sind Geräte zwar draußen im Einsatz, aber nicht zentral verwaltet. Updates laufen uneinheitlich, Berechtigungen sind zu breit, und es ist unklar, wie bei Verlust oder Verdachtsfällen reagiert wird. Ein zweiter Fehler ist, dass Vernetzung nur unter Performance-Aspekten gesehen wird, nicht unter Sicherheits- und Verfügbarkeitsaspekten. Und ein dritter Punkt: Support wird unterschätzt. Technische Lösung allein reicht nicht, wenn im Ernstfall niemand erreichbar ist oder Zuständigkeiten fehlen. Genau deshalb ist die Verbindung aus Vernetzung, Gerätemanagement und 24/7-Unterstützung heute so relevant.

Security wird oft als reine Schutzmaßnahme verstanden. Wo sehen Sie den Punkt, an dem Sicherheit auch zu einem wirtschaftlichen Faktor wird — also zu einem Hebel für Stabilität, Vertrauen und Wettbewerbsfähigkeit?

Sobald Sicherheit darüber entscheidet, ob ein Unternehmen arbeitsfähig bleibt, wird sie zum wirtschaftlichen Faktor. Wenn Systeme ausfallen, Kommunikation unterbrochen ist oder Daten nicht verfügbar sind, ist das kein IT-Problem mehr, sondern ein unmittelbares Geschäftsrisiko: Umsatzausfall, Produktivitätsverlust, Vertrauensverlust bei Kunden und Partnern. Sicherheit ist daher nicht nur Abwehr, sondern eine Voraussetzung für stabile Prozesse, verlässliche Services und professionelle Außenwirkung. Unternehmen, die sicher und resilient arbeiten, sind in der Praxis oft auch schneller, vertrauenswürdiger und belastbarer.

Wie stark ist das Bewusstsein dafür gewachsen, dass Ausfallsicherheit, Datenverfügbarkeit und geschützte Kommunikation heute ebenso entscheidend sind wie klassische Cyberabwehr?

Das Bewusstsein ist klar gewachsen, aber in der Praxis noch nicht überall gleich stark verankert. Viele Unternehmen haben verstanden, dass Security heute mehr ist als klassischer Virenschutz. Gleichzeitig sehen wir, dass Abwehrmaßnahmen oft noch höher priorisiert werden als Themen wie Verfügbarkeit, sichere Vernetzung oder Reaktionsfähigkeit im Störungsfall. Gerade für Business-Kunden ist aber genau dieses Gesamtbild entscheidend: Schutz vor Angriffen – ja, aber ebenso die Fähigkeit, standortübergreifend sicher zu arbeiten und im Ernstfall schnell wieder handlungsfähig zu sein. Dabei geht es zunehmend um ein Zusammenspiel entlang der gesamten Verbindungskette. Netzbasierte Sicherheitslösungen wie Internetschutz Pro können hier einen wichtigen Beitrag leisten, indem sie Bedrohungen bereits im Netzwerk erkennen und blockieren und damit sowohl Sicherheit als auch Stabilität im laufenden Betrieb unterstützen.

Welche Rolle spielt dabei ein Anbieter wie Drei? Reicht es heute noch, Konnektivität bereitzustellen, oder erwarten Unternehmen längst integrierte Lösungen, die Vernetzung, Schutz und Support zusammendenken?

Nur Konnektivität bereitzustellen, reicht aus meiner Sicht heute nicht mehr. Unternehmen erwarten zunehmend, dass ein Partner mehr kann als Leitung und Tarif. Gefragt sind integrierte Lösungen: sichere Vernetzung, Schutz vor digitalen Bedrohungen, zentrale Verwaltung mobiler Geräte und ein Supportmodell, auf das man sich verlassen kann. Genau so positioniert sich Drei auf der Business-Seite: mit Vernetzungslösungen, Internetschutz Pro, Mobile Device Management und je nach Bedarf auch Lösungen mit mehr Kontrolle und Sicherheit wie Private Network.

Wenn Sie einem KMU drei konkrete Prioritäten nennen müssten, um die eigene Sicherheitsstrategie zukunftsfähig aufzustellen: Welche wären das – und wo kann Drei dabei ganz konkret unterstützen?

1. Basis-Schutz standardisieren. Jedes KMU braucht heute ein belastbares Sicherheits-Grundniveau: Schutz vor schädlichen Seiten, Malware, Ransomware, Software-Schwachstellen und idealerweise auch Warnmechanismen bei verdächtigen Aktivitäten. Hier kann Drei mit Internetschutz Pro unterstützen, das netzbasierten Schutz mit Geräteschutz kombiniert.
2. Mobile Geräte professionell verwalten. Smartphones, Tablets und Laptops sind längst kritische Business-Endgeräte. Deshalb sollten Unternehmen Geräte zentral verwalten, Sicherheitsupdates steuern, private und geschäftliche Daten trennen und bei Verlust sperren oder löschen können. Genau dafür bietet Drei mit Miradore Mobile Device Management eine passende Lösung.
3. Sicherheit operativ absichern mit klaren Zuständigkeiten und stabiler Vernetzung. Im Ernstfall zählt nicht nur die Technologie, sondern vor allem, wie schnell und strukturiert reagiert wird. Unternehmen sollten daher klare Verantwortlichkeiten definieren und sicherstellen, dass ihre Vernetzung stabil und verlässlich funktioniert. Drei kann hier unterstützen, indem sichere Konnektivität und einfach integrierbare Sicherheitslösungen bereitgestellt werden, die im Alltag funktionieren und im Störungsfall keine zusätzliche Komplexität erzeugen.

ZENTRALE BEGRIFFE DER DIGITALEN SICHERHEIT

Digitale Sicherheit ist ein vielschichtiges Thema, das im Unternehmensalltag zunehmend an Bedeutung gewinnt. Gleichzeitig wird sie oft von einer Vielzahl an Fachbegriffen begleitet, die unterschiedliche Bedrohungen und Schutzmechanismen beschreiben. Um Risiken richtig einschätzen und geeignete Maßnahmen ableiten zu können, ist ein grundlegendes Verständnis dieser Begriffe entscheidend.

Die wichtigsten Begriffe rund um digitale Sicherheit im Überblick:

- **Malware & Ransomware**
  Malware und Ransomware zählen zu den häufigsten Formen digitaler Angriffe. Während Malware als Sammelbegriff für schädliche Software gilt, die Systeme beschädigen oder Daten stehlen kann, bezeichnet Ransomware eine spezifische Variante, bei der Daten verschlüsselt und anschließend zur Erpressung genutzt werden.

- **Social Engineering**
  Dabei werden keine technischen Schwachstellen ausgenutzt, sondern Menschen gezielt manipuliert – etwa durch gefälschte E-Mails oder täuschend echte Kommunikationsversuche – um an vertrauliche Informationen wie Passwörter oder Zugangsdaten zu gelangen.

- **MDM**
  Ein weiterer zentraler Bereich ist das Mobile Device Management (MDM). Dabei handelt es sich um Lösungen, mit denen Unternehmen mobile Endgeräte wie Smartphones, Tablets und Laptops zentral verwalten, absichern und im Ernstfall auch aus der Ferne sperren oder löschen können.

drei.at


Standort-
Vernetzung:
sicher & leicht
gemacht.
Unser anpassungsfähiges
SD-WAN für überall, wo es
Internet gibt.
Für jede
Standort-
Größe
Jetzt
Beratung
vereinbaren!
drei.at/sdwan
Business

Resilienz beginnt vor der Krise

Teresa Loreth von Detecon zeigt auf, warum Business Continuity Management heute über IT hinausdenken muss – und Unternehmen oft erst in der Krise erkennen, wo ihre wahren Schwachstellen liegen.

Text: Philipp Josef Rossmann

Krisen gehören längst zum Betriebsalltag – und doch zeigt sich im Ernstfall immer wieder, wie lückenhaft die Vorbereitung vieler Unternehmen ist. Zwischen formal vorhandenen Notfallplänen und tatsächlicher Handlungsfähigkeit klafft oft eine entscheidende Lücke. Während Risiken erkannt werden, bleiben wirksame Maßnahmen häufig aus oder greifen zu kurz. Im Gespräch erklärt Teresa Loreth von Detecon, warum klassische Sicherheitslogiken heute nicht mehr ausreichen, wo die größten blinden Flecken liegen und weshalb echte Resilienz weit über IT-Schutz hinausgeht. Sie plädiert für einen pragmatischen, ganzheitlichen Zugang zu Business Continuity Management, der nicht nur interne Prozesse, sondern auch Abhängigkeiten, Szenarien und das konkrete Handeln im Krisenfall in den Mittelpunkt stellt.

Viele Unternehmen glauben, sie seien auf Krisen gut vorbereitet – bis der erste echte Ausfall eintritt. Wo erleben Sie in der Praxis die größten blinden Flecken, die Unternehmen selbst oft nicht auf dem Radar haben?

In der Praxis zeigt sich, dass zu wenig geübt und zu wenig ehrlich hinterfragt wird, was tatsächlich kritisch ist und im Ernstfall unbedingt funktionieren muss. Viele Organisationen verlassen sich auf Pläne, die gut aussehen, aber nie unter realistischen Bedingungen getestet wurden. Hinzu kommt ein veraltetes Bedrohungsbild: Wir leben längst nicht mehr auf der sprichwörtlichen „bunten Blumenwiese". Sabotage, Manipulation, Desinformationskampagnen und geopolitische Verwerfungen sind keine Ausnahmen mehr, sondern Teil des Normalzustands. Zwar werden Risiken oft erkannt – die Maßnahmen greifen jedoch häufig am Problem vorbei. Covid hat das sehr deutlich gezeigt: Händewaschen war sichtbar und einfach, verfehlte aber die eigentlichen Herausforderungen wie Remote Work, digitale Prozesse oder rechtssichere elektronische Signaturen. Genau diese Diskrepanz zwischen erkanntem Risiko und wirksamer Maßnahme ist einer der größten blinden Flecken.

> **„Resilienz beginnt genau in dem Moment, in dem klassische Cyber-Security endet – wenn Unternehmen trotz eingeschränkter Systeme und Zeitdruck handlungsfähig bleiben müssen.**
>
> **Teresa Loreth**

Wenn von Business Continuity Management die Rede ist, denken viele zuerst an IT-Notfälle. Tatsächlich reicht das Spektrum aber von Stromausfällen über Lieferkettenprobleme bis zu geopolitischen Krisen. Wie breit muss BCM heute gedacht werden?

BCM muss heute ganzheitlich gedacht werden: Es geht darum, alle internen und externen Bedrohungen sowie deren Auswirkungen entlang der gesamten Wertschöpfungskette zu betrachten. Der Fokus allein auf interne Prozesse reicht in einer vernetzten Welt nicht mehr aus – entscheidend sind auch Abhängigkeiten von Lieferanten und kritischen Abnehmern.

Ab wann sollte sich ein Unternehmen ernsthaft mit Business Continuity Management beschäftigen: erst ab einer gewissen Größe, ab regulatorischem Druck – oder idealerweise viel früher?

Ich bin ein klarer Verfechter pragmatischer Ansätze und schneller, wirksamer Lösungen. Nicht jedes Unternehmen braucht automatisch ein vollständiges BCM-System. Oft genügt eine ehrliche Kernfrage: Was ist in meinem Unternehmen wirklich kritisch – und was muss im Ernstfall zumindest eingeschränkt weiterlaufen können? Genau dieser „Degraded Mode" ist häufig der entscheidende Hebel für Handlungsfähigkeit.

Gibt es typische Schwachstellen, die sich branchenübergreifend wiederholen – also Bereiche, in denen Unternehmen ihre eigene Verwundbarkeit systematisch unterschätzen?

Ein typisches Muster ist, dass sich der Fokus stark auf die IT verengt. In der Praxis betreuen wir sowohl die Business-Seite (BCM) als auch die IT-Perspektive (IT Service Continuity Management). Beides getrennt zu betrachten greift zu kurz: Ohne das Zusammenspiel von Business und IT bleibt die Absicherung unvollständig. Ich spreche dann gerne von einer „halben Resilienz" – und die hilft im Ernstfall niemandem.

Sie identifizieren mit Unternehmen konkrete Ausfallrisiken. Wie geht man dabei methodisch vor: Beginnt man bei den kritischsten Prozessen, bei technischen Abhängigkeiten oder bei externen Faktoren wie Energie, Software-Anbietern oder geopolitischen Spannungen?

Wir gehen dabei bewusst schrittweise vor. Zuerst geht es darum, ein klares Bild zu schaffen, was im Unternehmen wirklich kritisch ist. Sind es einzelne Kernprozesse – oder stehen am Ende sogenannte Endservices, die für Kunden essenziell sind? Ist diese Frage beantwortet, folgt der Blick auf die interne und externe Gefahrenlage. Aus ihr lassen sich relevante Bedrohungen und realistische Szenarien ableiten. Genau diese Szenarien bilden dann die Grundlage für praxistaugliche Notfallpläne und schnelle, wirksame Maßnahmen für den Ernstfall.

Viele Betriebe haben Notfallpläne in der Schublade, aber selten realitätsnahe Übungen. Wie wichtig sind BCM-Tests, Krisensimulationen und Events, um aus einem Papierkonzept tatsächlich Handlungsfähigkeit zu machen?

Das A und O eines gut gemanagten Ereignisses ist die konsequente Vorbereitung – und vor allem das regelmäßige Üben. In der Praxis sehen wir, dass Organisationen erst durch realistische Krisensimulationen wirklich handlungsfähig werden. Deshalb begleiten wir unsere Kunden intensiv bei Kri-

senübungen, beim Aufbau funktionierender Krisenstäbe und beim Durchspielen realistischer Szenarien – bis hin zur konkreten Tagung des Krisenstabs im simulierten Ernstfall.

Wo endet klassische Cyber-Security und wo beginnt echte Resilienz? Anders gefragt: Was muss zusätzlich passieren, damit ein Unternehmen nicht nur Angriffe abwehrt, sondern auch unter Stress arbeitsfähig bleibt?
Dort, wo der Angriff trotz aller Schutzmaßnahmen erfolgreich war. Echte Resilienz beginnt genau in diesem Moment. Sie entscheidet, ob ein Unternehmen unter Stress weiterarbeiten kann – wenn Systeme eingeschränkt sind, Informationen unvollständig und Entscheidungen unter Zeitdruck getroffen werden müssen. Dafür braucht es mehr als technische Abwehr: klare Prioritäten, trainierte Rollen, eingeübte Entscheidungsprozesse und praxistaugliche Notfall- und Wiederanlaufpläne. Resilienz heißt nicht, jeden Angriff zu verhindern, sondern auch dann handlungsfähig zu bleiben, wenn es ernst wird.

Ein besonders heikler Punkt sind Abhängigkeiten von Dritten – etwa Cloud-Anbietern, Softwareplattformen oder internationalen Dienstleistern. Wie stark unterschätzen Unternehmen heute das Risiko, dass ein externer Ausfall den eigenen Betrieb unmittelbar lahmlegt?
Leider sehr stark. Viele Unternehmen denken noch zu sehr in ihren internen Silos und zu wenig „out of the box". Dabei sind Abhängigkeiten von Dritten in einer global vernetzten Welt längst Teil des Alltags – und damit auch ein zentraler Risikofaktor, der in Risikoanalysen oft zu wenig berücksichtigt wird. Genau hier setzen wir mit unserem Resilienz-Framework an: mit einer ganzheitlichen BCM-Methodik, die nicht nur die eigenen Prozesse betrachtet, sondern Supplier am Anfang der Kette ebenso einbezieht wie Kunden am Ende. Ergänzend helfen digitale Souveränitätsanalysen, Abhängigkeiten sichtbar zu machen und realistisch zu bewerten.

Mit dem NISG 2026 kommen in Österreich ab 1. Oktober 2026 für viele betroffene Unternehmen neue Pflichten rund um Sicherheitsmaßnahmen und die Meldung erheblicher Vorfälle. Was bedeutet dieses Gesetz aus Ihrer Sicht praktisch für Unternehmen – und wo sehen Sie derzeit den größten Aufholbedarf?
Ich sehe das NIS-2-Gesetz klar als Chance für betroffene Unternehmen, sich strukturierter mit Cyber-Sicherheitsanforderungen auseinanderzusetzen. Cyberbedrohungen zählen – neben geopolitischen Entwicklungen und der Klimakrise – aus meiner Sicht nach wie vor zu den am meisten unterschätzten Risikofaktoren. Gleichzeitig ist nicht zu übersehen, dass mit NISG, RKEG und weiteren Vorgaben eine Vielzahl neuer regulatorischer Anforderungen auf Unternehmen einwirkt und der bürokratische Druck zunimmt. Der eigentliche Mehrwert entsteht jedoch nur dann, wenn Unternehmen bei der Umsetzung aktiv begleitet werden und der Gesetzgeber praxisnahe, verständliche Leitlinien bereitstellt.

Gibt es so etwas wie ein sinnvolles Standardpaket für BCM und Resilienz – oder ist jedes Unternehmen gezwungen, seine eigene Sicherheitsarchitektur individuell zu entwickeln?
Ja, die Vorgehensweise ist im Kern ähnlich: Kritikalitäten klären, relevante Bedrohungen identifizieren, realistische Szenarien entwickeln und daraus praxistaugliche Notfallmaßnahmen ableiten und verankern. Entscheidend ist dabei, die Pragmatik nicht aus den Augen zu verlieren. Resilienz entsteht nicht durch überkomplexe Konzepte, sondern durch Lösungen, die umsetzbar sind und von den Mitarbeitenden im Alltag tatsächlich gelebt werden. Krisen und Notfälle werden uns auch künftig intensiv begleiten – Business Continuity Management hilft jedoch dabei, ihnen strukturiert, handlungsfähig und mit deutlich mehr Souveränität zu begegnen – und den Weg durch den Ernstfall zumindest etwas entspannter zu gestalten.

INFOBOX

Detecon ist eine führende Management- und Technologieberatung mit Fokus auf digitaler Transformation. Als eigenständiges Unternehmen im Konzernverbund der Deutschen Telekom ist digitale Kompetenz ein fester Bestandteil der Unternehmens-DNA. Mit mehr als 140 Mitarbeitenden an den Standorten Wien und Zürich sowie einem internationalen Netzwerk gestaltet Detecon gemeinsam mit Kunden den Weg zur digitalen Exzellenz.

Das Beratungsportfolio gliedert sich in die Bereiche Technologie, Strategie und Business, wobei Themen wie Enterprise Architecture, Business Process Management, Cyber-Security, Data Excellence und Change Management branchenübergreifend relevant sind.

Neben dem Fokus-Thema Resilienz stehen 2026 noch folgende weitere Kern-Areas bei Detecon im Fokus:

- **AI Use Cases**
  Im Fokus stehen skalierbare, geschäftsrelevante KI-Anwendungen, die im Einklang mit Governance-Vorgaben messbaren Mehrwert schaffen.
- **IT Service Costing**
  Ein integrierter Ansatz, der IT-Kostenmanagement, Cloud FinOps und Technology-ROI verbindet und Business, IT sowie Finance über gemeinsame Steuerungsgrößen zusammenführt.
- **Digital Planning mit GenAI**
  Automatisierte Abweichungserkennung, laufende Rolling Forecasts auf Basis aktueller Ist-Daten und Szenarien, die sich in Minuten statt Tagen modellieren lassen, verändern die klassischen Forecastingprozesse grundlegend.
- **Digitale Souveränität**
  Digitale Souveränität verbindet technologische Unabhängigkeit, Sicherheit, Compliance und Innovationsfähigkeit. Ziel ist es, Unternehmen von reinen Nutzern zu aktiven Gestaltern digitaler Systeme zu entwickeln.

detecon.com

Liechtenstein
FINANCE

Warum Rechtssicherheit zählt

Verlässlichkeit, Vorhersehbarkeit und Stabilität eines Rechtssystems sind Faktoren, die für Kunden, Investoren, Vermögensverwalter und Unternehmen von essentieller Bedeutung sind. Denn wer Kapital langfristig anlegt oder komplexe Strukturen aufsetzt, ist darauf angewiesen, dass gesetzliche Rahmenbedingungen nicht nur klar formuliert, sondern auch konsistent angewendet und nachhaltig ausgestaltet sind.

Mangelnde Rechtssicherheit führt nicht nur zu mangelnder Planungssicherheit. Unklare Vorschriften, häufige Gesetzesänderungen oder eine uneinheitliche Rechtsprechung schmälern die Attraktivität von Investitionen und von Finanzplätzen. Gerade im internationalen Kontext, wenn Vermögen grenzüberschreitend strukturiert werden soll, suchen Kunden gezielt nach Standorten mit einem stabilen, transparenten Rechtsrahmen, an denen sie sich auf die Durchsetzbarkeit ihrer Rechte verlassen können. Es muss morgen noch gelten, worauf Kunden heute vertrauen.

Ein (rechts-)sicherer Hafen für Kapital

Liechtenstein hat sich in diesem Zusammenhang als besonders verlässlicher Finanzplatz etabliert. Das Fürstentum bietet ein modernes, klar strukturiertes und zugleich flexibles Rechtssystem, das sich an internationalen Standards orientiert und gleichzeitig Kontinuität gewährleistet. Gesetzesänderungen erfolgen wohlüberlegt und unter Einbezug von Experten sowie Marktteilnehmern, was zu einer hohen Akzeptanz und Praxistauglichkeit führt. Die konsequente Rechtsentwicklung bildet in Kombination mit der ausgeprägten politischen Stabilität und liberalen Wirtschaftsordnung den idealen Rahmen für den (auch grenzüberschreitenden) Vermögensschutz über Generationen hinweg.

Regulatorische Balance

Hinzu kommt die enge Einbindung Liechtensteins in den europäischen Wirtschaftsraum. Dadurch profitieren Marktteilnehmer von einem harmonisierten Rechtsrahmen und gleichzeitig von den spezifischen Vorteilen eines kleinen, effizienten Staates. Behörden und Gerichte arbeiten schnell und praxisnah, was die Umsetzung rechtlicher Anliegen erleichtert. Diese Effizienz stärkt das Vertrauen in die Institutionen und erhöht die Attraktivität des Standorts zusätzlich. Liechtenstein verfolgt eine ausgewogene Strategie: Einerseits werden internationale Vorgaben konsequent umgesetzt, andererseits wird darauf geachtet, die Wettbewerbsfähigkeit des Finanzplatzes zu erhalten. Diese Balance sorgt dafür, dass Marktteilnehmer sowohl regulatorische Klarheit als auch unternehmerische Freiheit genießen.

Entscheidender Wettbewerbsvorteil

Der Finanzplatz Liechtenstein verfügt im Bereich der Vermögensverwaltung und -strukturierung über eine lange Tradition und hohe Expertise. Die entsprechenden unverzichtbaren gesetzlichen Grundlagen sind klar definiert und international anerkannt, was Rechtssicherheit auch in komplexen Sachverhalten gewährleistet. So bildet etwa das liechtensteinische Personen- und Gesellschaftsrecht seit nunmehr genau 100 Jahren, sprich seit 1926, das gesetzliche Fundament des Finanzplatzes. Liechtenstein gelingt es in besonderer Weise, Stabilität, Transparenz und Innovationsfähigkeit miteinander zu verbinden. Gerade in einer zunehmend komplexen und dynamischen globalen (Finanz-)Welt stellt dies einen entscheidenden Wettbewerbsvorteil dar.

INFOBOX

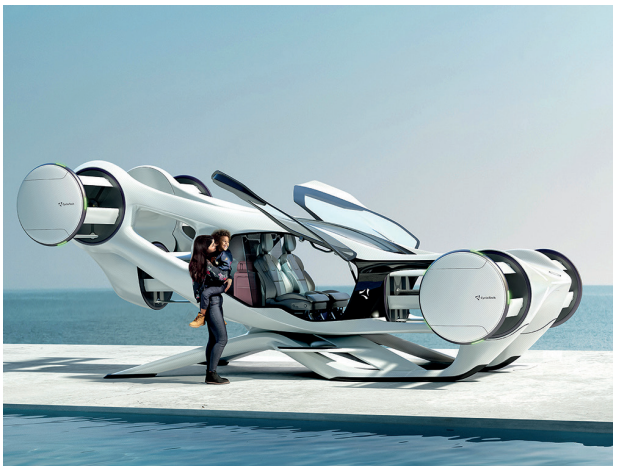
Liechtenstein Finance e.V. ist ein privatrechtlich organisierter Verein, dessen Mitglieder die Regierung des Fürstentums Liechtenstein und die liechtensteinischen Finanzplatzverbände sind. Zweck des Vereins ist es, das Profil des liechtensteinischen Finanzplatzes im In- und Ausland durch Informationsarbeit zu den Besonderheiten und Stärken des Standortes zu schärfen.

finance.li

Ideen mit Vorsprung

Sechs Unternehmen, sechs Bereiche – ein gemeinsamer Nenner: Technologie, die Geschäftsmodelle konkret macht. Von der Luftfahrt über den Wohnbau bis hin zum Recycling versammeln wir Akteure, die Märkte neu denken und die Zukunft operativ gestalten.

Text: Philipp Josef Rossmann



1

Präzision hebt ab

Das Linzer Hightech-Unternehmen CycloTech GmbH treibt die Entwicklung der elektrischen Luftfahrt voran. Mithilfe des CycloRotor-Systems ermöglichen emissionsfreie VTOL-Fluggeräte eine 360°-Schubvektorsteuerung und sind somit präzise, wendig und für Schwebe- sowie Vorwärtsflüge geeignet. Nach dem Erstflug des BlackBird-Demonstrators und der Eröffnung neuer Standorte in München und Abu Dhabi fokussiert sich das Scale-up auf den Zukunftsmarkt „Advanced Air Mobility".

cyclotech.aero

2

Wohnbau, neu gedacht

GROPYUS industrialisiert den Wohnbau: Das in Wien ansässige Unternehmen realisiert schlüsselfertige Mehrfamilienhäuser in nachhaltiger Holzbauweise, von der digitalen Planung bis zur Übergabe. Herzstück ist eine Smart Factory mit roboterbasierter Serienfertigung. Ergänzt wird das Modell durch ein digitales Gebäudebetriebssystem für Verwaltung, Kosten und Rendite.

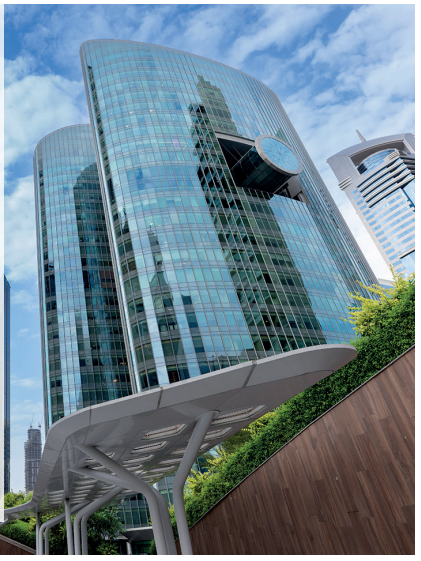
gropyus.com

3
CO_2 als Aufgabe

Das Schweizer Unternehmen Climeworks zählt zu den Pionieren im Bereich der CO_2-Entfernung aus der Atmosphäre. Mithilfe sogenannter Direct-Air-Capture-Anlagen filtert das Unternehmen Kohlenstoffdioxid direkt aus der Luft und speichert es dauerhaft im Untergrund oder führt es industriellen Anwendungen zu. Gegründet als Spin-off der ETH Zürich, betreibt Climeworks heute mehrere Anlagen, darunter großskalige Projekte in Island. Die Technologie gilt als vielversprechender Baustein im Kampf gegen den Klimawandel – insbesondere zur Kompensation schwer vermeidbarer Emissionen. **climeworks.com**

4
Finanzschnittstelle

Die liechtensteinische Privatbank Bank Frick positioniert sich als Schnittstelle zwischen klassischem Banking und digitaler Innovation. Das seit 1998 familiengeführte Institut hat sich auf Finanzintermediäre, Fintechs und professionelle Anleger spezialisiert. Als einer der europäischen Vorreiter im Bereich reguliertes Blockchain-Banking verbindet die Bank traditionelle Finanzexpertise mit zukunftsorientierten Technologien – und expandiert mit einem neuen Standort in Dubai (Bild) gezielt in internationale Wachstumsmärkte. **bankfrick.li**

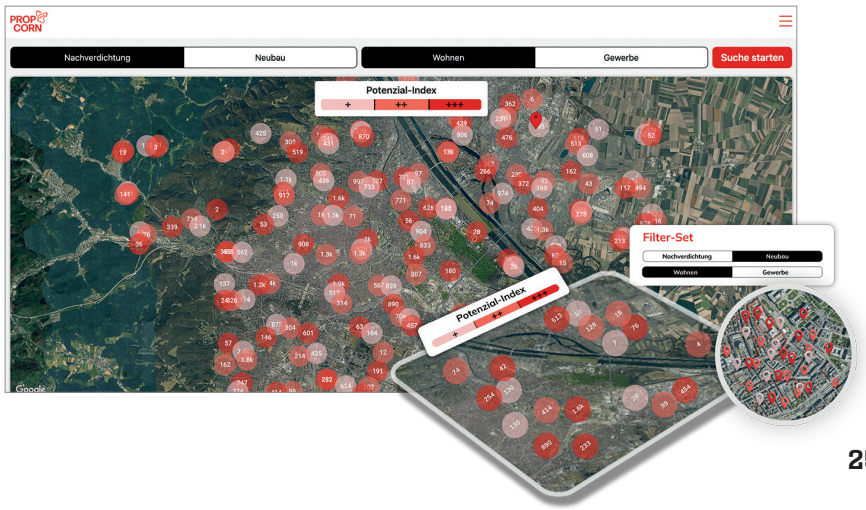


5
Recycling, neu codiert

Weltweit wird mehr als 90 Prozent des Plastiks nicht recycelt. DePoly will das ändern und sorgt dafür, dass Abfall wieder zum Rohstoff wird, indem das chemische Recycling industriell umgesetzt wird. Das Schweizer Cleantech-Unternehmen verwandelt schwer recycelbare PET- und Polyesterabfälle in hochwertige Monomere und führt sie zurück in den Materialkreislauf – genau dort, wo bestehende Systeme an ihre Grenzen stoßen. Mit Hauptsitz in Sion und einer Showcase-Anlage in Monthey konzentriert sich DePoly auf jene Abfälle, an denen klassisches Recycling bislang scheiterte. **depoly.co**

6
Immobilien in Echtzeit

Eine KI-Suchmaschine für Off-Market-Deals: PROPCORN AI verschiebt Immobilienanalyse von der Schätzung zur Echtzeitentscheidung. Das 2024 gegründete Wiener Unternehmen nutzt künstliche Intelligenz, um Baupotenziale, Nachverdichtung, Neubauoptionen und Portfolio-Chancen auf Basis von Flächenwidmung und Baubestimmungen in Sekunden sichtbar zu machen – für Entwickler, Banken, Makler, Städte und Investoren. **propcorn.ai**



Schutzschild gegen Cyberangriffe

In einer zunehmend digitalisierten Welt, in der nahezu alle Geschäftsprozesse, Kommunikationswege und Datenflüsse über vernetzte Systeme laufen, gewinnt das Thema Cybersicherheit eine immer zentralere Bedeutung. **Text:** Martin Wechtl

Unternehmen, Behörden und Institutionen sehen sich einer stetig wachsenden Bedrohung durch hochprofessionelle und spezialisierte Cyberkriminelle ausgesetzt. Diese agieren oft in gut organisierten Strukturen, entwickeln immer raffiniertere Angriffsmethoden und sind technisch häufig auf dem neuesten Stand. Ihre Intention ist es, unbemerkt in IT-Systeme einzudringen, Schadsoftware zu platzieren, vertrauliche Informationen zu entwenden und daraus finanziellen Profit zu schlagen. Die daraus resultierenden Schäden können nicht nur enorme finanzielle Verluste verursachen, sondern im schlimmsten Fall sogar die Existenz eines Unternehmens gefährden.

Die Agentur Cyberschutz – Cyber- und IT-Security & Consulting GmbH hat es sich zur Aufgabe gemacht, genau diesen Gefahren entgegenzuwirken und Unternehmen bestmöglich gegen digitale Angriffe zu schützen. Im Mittelpunkt steht ein ganzheitlicher, mehrschichtiger Ansatz, der sowohl präventive Maßnahmen als auch professionelle Unterstützung im Schadensfall umfasst. Das interdisziplinäre Team aus IT-Experten, Kriminalisten und Analysten wertet täglich aktuelle Bedrohungen aus und erstellt detaillierte Täterprofile. Ziel ist es, Organisationen aller Größen und Branchen angesichts steigender Cyberrisiken nachhaltig zu schützen.

Basierend auf aktuellen Angriffsmethoden und Bedrohungslagen bietet die Agentur spezialisierte Leistungen in vier zentralen Bereichen an. Der erste Bereich umfasst die interne IT-Security, darunter Remote Monitoring und Management (RMM), kontinuierliche Schwachstellenanalysen (CVE Scans), Endpoint Detection and Response (MDR) sowie Multi-Faktor-Authentifizierung (MFA). Diese Maßnahmen stärken die Sicherheitsstruktur innerhalb der Organisation.

Die zweite Kategorie betrifft die externe IT-Security. Hierzu zählen unter anderem SecureDNS-Lösungen, Darknet-Monitoring, Attack Surface Management sowie

externe Schwachstellenanalysen. Zweck ist es, potenzielle Risiken außerhalb der eigenen Infrastruktur frühzeitig zu erkennen und zu minimieren.

Ein weiterer wichtiger Bestandteil ist der Bereich Vorträge und Cyber-Schulungsplattformen. Die Agentur vermittelt praxisnahes Wissen zu Themen wie Cybercrime, Darknet, IT-Sicherheit und Täterverhalten. Geschäftsführer und Gründer Oliver Hietz bringt als ehemaliger Kriminalpolizist umfangreiche Erfahrung in der Analyse von Straftaten, insbesondere im Bereich Cyberkriminalität, mit. Dieses Wissen fließt direkt in die Schulungskonzepte ein und ermöglicht praxisnahe Einblicke in die Denk- und Vorgehensweisen von Tätern – ein absolutes Alleinstellungsmerkmal. Die Teilnehmer profitieren von realitätsnahen Szenarien und lernen, potenzielle Gefahren frühzeitig zu erkennen und richtig zu reagieren. Dies stärkt nicht nur die individuelle Kompetenz, sondern erhöht auch die Sicherheitskultur innerhalb des gesamten Unternehmens.

Der vierte Bereich ist der Incident Response Service, der im Ernstfall – also einem erfolgreichen Hackerangriff – zum Einsatz kommt. In einer solchen Ausnahmesituation zählt jede Minute, weshalb ein eingespieltes Team bereitsteht, um schnell, strukturiert und effizient zu reagieren. Es unterstützt die Betroffenen nicht nur bei der technischen Bewältigung des Angriffs, etwa bei der Analyse von Schadsoftware oder der Wiederherstellung von Systemen, sondern begleitet sie auch strategisch und organisatorisch durch den gesamten Schadensfall. Dazu gehören unter anderem Kommunikationsmaßnahmen, rechtliche Abstimmungen sowie die Koordination mit relevanten Partnern. Dabei geht es darum, die Auswirkungen so gering wie möglich zu halten und den Geschäftsbetrieb schnellstmöglich wiederherzustellen.

Die Dienstleistungen sind auf regulatorische Anforderungen wie NIS-2 und DORA ausgerichtet. Dies umfasst insbesondere die Einhaltung von IT-Sicherheitsstandards sowie die Überprüfung von Partnern und Lieferketten. Zusätzlich unterstützt die Agentur Unternehmen bei der Erfüllung und dem Nachweis von Voraussetzungen für Cyberversicherungen.

Doch auch die besten Sicherheitsmaßnahmen sind wirkungslos, wenn das Bewusstsein für die Gefahr fehlt. Für Oliver Hietz steht fest, dass der Mensch eine entscheidende Rolle im Kampf gegen Cyberkriminalität spielt. Technische Schutzmaßnahmen allein reichen nicht aus, wenn Mitarbeitende nicht ausreichend sensibilisiert und geschult sind. Häufig sind es menschliche Fehler, wie das unbedachte Öffnen von E-Mail-Anhängen oder das Klicken auf manipulierte Links, die Angreifern überhaupt erst den Zugang zu Systemen ermöglichen. Gleichzeitig sind Täter in ihrer Entwicklung oft mehrere Schritte voraus, da sie flexibel agieren und nicht an bestehende Strukturen oder Regularien gebunden sind. Veraltete Sicherheitsstrategien wie einfache Passwortsysteme, einmalige Penetrationstests oder standardisierte Zwei-Faktor-Authentifizierungen reichen daher nicht mehr aus, um modernen Bedrohungen wirksam zu begegnen.

Aus diesem Grund setzt die Agentur auf zeitgemäße, dynamische Lösungen, die kontinuierlich weiterentwickelt und an aktuelle Bedrohungslagen angepasst werden. Dabei spielen Innovation, Anpassungsfähigkeit und eine enge Zusammenarbeit mit den Kunden eine entscheidende Rolle. Angestrebt wird, ein Gleichgewicht zwischen Angreifern und Verteidigern herzustellen und Unternehmen in die Lage zu versetzen, nicht nur zu reagieren, sondern proaktiv auf neue Risiken zu antworten. Langfristig besteht die Hoffnung, dass durch ein hohes Sicherheitsniveau, gezielte Aufklärung und konsequente Prävention Cyberkriminelle abgeschreckt werden und ihre Aktivitäten auf weniger geschützte Ziele verlagern. Gleichzeitig trägt ein solches Sicherheitsbewusstsein dazu bei, das Vertrauen von Kunden, Partnern und der Öffentlichkeit nachhaltig zu stärken und die digitale Zukunft sicherer zu gestalten.

Oliver Hietz ist Keynote Speaker, Cybercrime-Analyst und Gründer der Agentur Cyberschutz – Cyber- und IT-Security & Consulting GmbH. Bis 2024 im Polizeidienst tätig, gilt er als ausgewiesener Experte für Kriminalanalyse und Cybercrime-Delikte.

Agentur Cyberschutz

INFOBOX

Schützen Sie Ihr Unternehmen vor Cyberkriminalität mit der **Cyber-Risikoanalyse** der Agentur Cyberschutz!

Schon mit einem einzigen Klick lässt sich erkennen, an welchen Stellen Ihr Unternehmen potenziell anfällig für Cyberangriffe ist – kostenfrei und ohne Eingriff in Ihre IT-Systeme. Die Cyber-Risikoanalyse deckt Schwachstellen frühzeitig auf, noch bevor Angreifer diese ausnützen können, und liefert Ihnen konkrete Handlungsempfehlungen zur Verbesserung Ihrer Sicherheitsmaßnahmen. So sichern Sie nicht nur Ihre Daten und Ihren Ruf, sondern schaffen auch eine solide Grundlage für umfassenden Versicherungsschutz. Machen Sie mögliche Risiken sichtbar, bevor sie zum Problem werden!

QR-Code scannen und loslegen:

Digitale Souveränität beginnt beim Smartphone

Bei unserer 36. „Top Speakers Lounge“ am 6. Mai 2026 in Wien diskutierten Experten über digitale Abhängigkeiten, Datensouveränität und die unterschätzte Macht von Metadaten.

◀ v.l.n.r.: Susanne Bickel (Die Presse), Danilo Bargen (Threema GmbH), Univ.-Prof. Dr. Verena Dorner (WU Wien), Mag. Johann Weidlinger (PwC Legal)

▼ v.l.n.r.: Martin Schmid (PwC Austria), Mag. Johann Weidlinger (PwC Legal), Dr. Alexander Riklin (Präsident HKSÖL), Univ.-Prof. Dr. Verena Dorner (WU Wien), Susanne Bickel (Die Presse), Danilo Bargen (Threema GmbH), Dr. Rudolf Krickl (PwC Austria), Urs Weber (HKSÖL)

Cloud-Dienste aus den USA, KI-Modelle mit unklaren Trainingsdaten und Messenger-Plattformen, die umfassend Metadaten sammeln: Europas digitale Abhängigkeiten standen im Mittelpunkt der jüngsten „Top Speakers Lounge“ der Handelskammer Schweiz-Österreich-Liechtenstein (HKSÖL) in Wien. Unter dem Titel „Signalgate und BigTech-Abhängigkeit“ diskutierten Danilo Bargen vom Post-Quanten-Krypto-Messenger-Dienst Threema, Rechtsanwalt Mag. Johann Weidlinger (PwC Legal) und Univ.-Prof. Dr. Verena Dorner (WU Wien) über die Frage, wie Unternehmen und Privatpersonen die Kontrolle über ihre Daten zurückgewinnen können. Durch den Abend führte Susanne Bickel (Die Presse).

Mehr als nur Verschlüsselung

In seiner Keynote machte Danilo Bargen deutlich, dass digitale Souveränität weit über klassische Ende-zu-Ende-Verschlüsselung hinausgehe. Entscheidend sei vielmehr, wer Infrastruktur, Daten und Zugriffsmöglichkeiten kontrolliere. Der Schweizer Messenger-Dienst Threema setzt deshalb auf eigene Server in der Schweiz und verzichtet bewusst auf das Sammeln von Metadaten. „Erst die Kombination aus lückenloser Ende-zu-Ende-Verschlüsselung und Transparenz durch Open Source schafft das notwendige Vertrauen, um digitale Souveränität nachhaltig zu sichern“, so Bargen.

Die Telefonnummer als Schwachstelle

Besonders kritisch sieht Bargen die Rolle der eigenen Telefonnummer. Diese sei

▶ Beim anschließenden Get-together tauschten sich die Gäste der „Top Speakers Lounge“ in entspannter Atmosphäre weiter über technologische Entwicklungen und aktuelle Herausforderungen der digitalen Zukunft aus.

Mehr Impressionen:

▼ Das Publikum verfolgte die Diskussionen rund um digitale Souveränität, Datenschutz und Europas technologischen Abhängigkeiten bei der „Top Speakers Lounge“ mit großem Interesse.

längst mehr als nur eine Kontaktinformation. „An der Telefonnummer hängt viel: Wenn Sie sich bei WhatsApp anmelden, greift die App auf alle Kontakte zu“, erklärte er. Selbst Prepaid-Karten würden heute keine echte Anonymität mehr garantieren. Metadaten seien enorm mächtig – nicht umsonst stammt das bekannte Zitat „We kill people based on metadata“ vom ehemaligen CIA- und NSA-Direktor Michael Hayden. Digitale Souveränität müsse daher im Alltag gelebt werden – von Unternehmen ebenso wie von Privatpersonen.

Europas Abhängigkeit von US-Technologie

Auch aus juristischer Sicht seien die bestehenden Abhängigkeiten problematisch, erklärte Johann Weidlinger. Viele europäische Unternehmen hätten ihre Infrastruktur auf Anbieter aus Übersee aufgebaut. Gleichzeitig könnten US-Behörden unter bestimmten Voraussetzungen auf Daten zugreifen, ohne dass Betroffene davon erfahren. Orientierung biete hier unter anderem das EU Cloud Sovereignty Framework, das Kriterien zur Bewertung digitaler Abhängigkeiten definiert. Für Verena Dorner braucht es zusätzlich eine aktive europäische Förderpolitik. Viele souveräne Lösungen seien derzeit noch teurer als etablierte US-Angebote. Dennoch sieht sie Potenzial: Innerhalb der nächsten Jahre könnten europäische Alternativen entstehen, die technologisch konkurrenzfähig sind – allerdings mit stärkerem Fokus auf Datenschutz und Datensicherheit.

Zwischen USA und China

Im Zuge der Diskussion rückte auch China als möglicher Gegenspieler der US-Tech-Konzerne in den Fokus. Bargen verwies darauf, dass viele chinesische KI-Modelle mittlerweile offen zugänglich und lokal betreibbar seien – also unabhängig von externen Servern. Gleichzeitig warnte er jedoch vor fehlender Transparenz bei Trainingsdaten und möglichen neuen Abhängigkeiten. Auch Weidlinger plädierte für einen pragmatischen Zugang: Entscheidend sei weniger, ob Unternehmen ausländische Anbieter nutzen, sondern wie sie diese absichern. Denn digitale Souveränität dürfe letztlich nicht zulasten der wirtschaftlichen Wettbewerbsfähigkeit gehen.

ÜBER DIE „TOP SPEAKERS LOUNGE“

Die Plattform „Top Speakers Lounge“ ist eine Veranstaltungsreihe der Handelskammer Schweiz-Österreich-Liechtenstein (HKSÖL). Thematisiert werden aktuelle Entwicklungen in Wirtschaft und Politik. Zu den bisherigen Keynote Speakern zählen u. a. Roland Hunziker vom World Business Council for Sustainable Development (WBCSD), Karl Pall (Digitalisierungsexperte, Gründer Google Österreich), Medienmanager Rudi Klausnitzer, Marie-Gabrielle Ineichen-Fleisch (Staatssekretärin SECO der Eidgenossenschaft a. D.), Andreas Matthä (Vorstandsvorsitzender der ÖBB-Holding AG), Dr. Johannes Schweifer (Co-Founder Bitcoin Suisse AG), Peter Spuhler (Executive Chairman und Group CEO a. i. von Stadler Rail AG), Alexandra Reinagl (CEO der Wiener Linien), Wolfgang Mazal (Institut für Arbeits- und Sozialrecht der Universität Wien).

hk-schweiz.at

Coffee Circle

Der 42. Friends 4 Friends Netzwerkabend vereinte Design, Kulinarik und inspirierenden Austausch.

Friends 4 Friends startete 2026 im Nespresso Atelier Wien und setzte die Reihe exklusiver Netzwerkabende fort. Am 9. März wurde die Location in der Wiener Innenstadt zum Treffpunkt für einen Abend voller Genuss und inspirierenden Austausch. In eleganter Atmosphäre, begleitet von süßen und herzhaften Köstlichkeiten, Kaffee und Signature Coffee Cocktails, bot das Nespresso Atelier den passenden Rahmen. Die Verbindung aus Design, Kulinarik und Begegnung verlieh dem Abend eine besondere Qualität. Entscheidungsträger und Vertreter unterschiedlicher Branchen nutzten die Gelegenheit, um sich in stilvollem Ambiente auszutauschen, neue Kontakte zu knüpfen und bestehende Netzwerke zu vertiefen. Es entstanden anregende Gespräche sowie Impulse für künftige Kooperationen.

Liebevoll gestaltete Details rundeten den Abend ab. In den Goodie Bags fanden sich unter anderem Espressotassen als Erinnerung an das Event. Der Abend unterstrich den Wert persönlicher Begegnungen und die Bedeutung direkter Gespräche für ein lebendiges Netzwerk. Das Nespresso Atelier Wien erwies sich als ideale Bühne für den Auftakt ins neue Friends 4 Friends-Jahr. Ein Dank gilt Nespresso und Nestlé sowie den Partnern Fluglinie People's, BTV Vier Länder Bank AG und KESCH Event & Promotion GmbH.

▼ v.l.n.r.: Wolfgang Layr, Karin Kreutzer und Stefan Artner beim Friends 4 Friends Netzwerkabend im Nespresso Atelier Wien

▼ v.l.n.r.: Elias Krevatin (Fluglinie People's), Florian Ziegler (KESCH Event & Promotion GmbH), Jutta Rinderer (Fluglinie People's), Urs Weber (HKSÖL), Thomas Perchthaler (BTV Vier Länder Bank AG), Sarah Huber (Nestlé), Stefan Trojer (Nespresso)

Mehr Impressionen

HKSÖL-VERANSTALTUNGEN

Unsere Veranstaltungen verbinden Wissen und Netzwerk. Referenten wählen wir gezielt nach den Bedürfnissen unserer Mitglieder und aktuellen Wirtschaftsthemen aus.

Sie treffen auf Wirtschaftsexperten, Manager, Unternehmer und tauschen Gedanken und Informationen aus.

Als Mitglied sind Sie zu allen laufenden Veranstaltungen eingeladen – und können auch eigene Formate initiieren oder von uns umsetzen lassen.

EVENT-VORSCHAU

Auf folgende Veranstaltungen dürfen sich HKSÖL-Mitglieder in diesem Frühjahr freuen:

- **Gerichtssaal Europa**
  Mock Trial
  zum Einheitspatentgericht
  15. Juni 2026
  Zürich

- **Vorzeigestandort Schwyz**
  Top Talk
  17. Juni 2026
  Linz

- **Friends 4 Friends**
  Netzwerkabend
  12. August 2026
  Wien

- **Cybercrime & Darknet**
  Webinar
  8. September 2026

- **Top Speakers Lounge**
  5. November 2026
  Wien

Weitere Veranstaltungen, Details und Anmeldung:

Neu im Direktionsrat

Der Direktionsrat der HKSÖL wird durch drei profilierte Persönlichkeiten mit internationaler Expertise und strategischem Weitblick verstärkt.

Ali Kulein
CEO, Lindt & Sprüngli (Austria) Ges.m.b.H.

Seit September 2022 ist Ali Kulein Chief Executive Officer der Lindt & Sprüngli (Austria) GmbH in Wien. Zuvor war er als General Manager für das Russlandgeschäft des Schweizer Premiumschokoladenherstellers verantwortlich und prägte dessen Marktposition maßgeblich. Internationale Erfahrung sammelte er in leitenden Funktionen bei SC Johnson, unter anderem in Deutschland, Neuseeland und der Türkei, mit Fokus auf Markenführung und Vertrieb. In Österreich setzt er gezielt auf die Inszenierung der Marke im stationären Handel, beispielsweise durch die Eröffnung des ersten Lindt-Flagship-Stores in Wien, der die Markenwelt erlebbar macht. Dank seiner langjährigen Expertise im internationalen FMCG-Umfeld steht Kulein für eine strategisch ausgerichtete Markenführung im Premiumsegment. Er ist für die Weiterentwicklung von Lindt sowie der Traditionsmarken Hofbauer und Küfferle verantwortlich.

Seit März 2026 ist Rainer Steinlesberger CEO von Zühlke Engineering Österreich. Er ist ein international erfahrener Manager mit Fokus auf Digitalisierung und IT-Services sowie einem tiefen Marktverständnis. In seiner Laufbahn hatte er Top-Management- und C-Level-Funktionen in globalen Technologiekonzernen sowie in von Private Equity geprägten Wachstumsumfeldern inne, zuletzt als Group Chief Sales Officer und Managing Director. Seine Vision ist es, mit Zühlke einen aktiven Beitrag zur technologischen Wettbewerbsfähigkeit Österreichs zu leisten – insbesondere in den Bereichen Industrie, öffentlicher Sektor, Energie und regulierte Märkte. Durch die Verbindung von Consulting und exzellenter IT-Kompetenz kann Zühlke Industrie, öffentliche Hand und regulierte Märkte ganzheitlich in die digitale Zukunft führen. Zühlke agiert dabei nicht als kurzfristiger Dienstleister, sondern als langfristiger Transformationspartner.

Rainer Steinlesberger
CEO Österreich, Zühlke Engineering AG

Dr. Claudio Passardi
CFO, Zürich Versicherungs AG Österreich

Dr. Claudio Passardi ist seit dem 1. Jänner 2026 Chief Financial Officer (CFO) der Zürich Versicherungs AG in Österreich. Bereits zuvor prägte er als Chief Investment Officer sowie in leitenden Funktionen im Bereich Asset Management und Controlling über viele Jahre hinweg die finanzielle Ausrichtung des Unternehmens maßgeblich. Internationale Erfahrung sammelte er zudem bei Farmers Business Insurance in Los Angeles, wo er im Finanzbereich tätig war. Seine Karriere bei der Zurich Gruppe begann er 2006 als Vorstandsassistent am Hauptsitz in Zürich, wo er früh an strategischen Projekten auf Konzernebene mitwirkte. Er studierte Betriebswirtschaft an der Universität Zürich, schloss 2002 mit einem Master ab und promovierte 2005. Der gebürtige Schweizer verfügt über umfassende Finanz- und Managementexpertise sowie sehr gute Sprachkenntnisse in Deutsch, Englisch, Französisch, Italienisch, Spanisch und Portugiesisch.

PRÄSIDIUM

Präsident
Dr. Alexander RIKLIN
Gesellschafter und Vorsitzender des Beirates, ALCAR Holding GmbH, Hirtenberg

Vizepräsident
Dipl.-Ing. Dr. Nikolaus KAWKA
Geschäftsführer, kawka3W Business Consulting, Wien

Vizepräsidentin
Angelika MOOSLEITHNER
Member of the Group Board, First Advisory Group, Vaduz

Vizepräsident
Michael PÉREZ lic. iur.
Partner, LAWCO. Rechtsanwälte | attorneys at law, Wien

EHRENPRÄSIDIUM

Ehrenpräsident
Dipl.-Ing. Heinz FELSNER
Gesellschafter, EFH Beteiligung GmbH

Ehrenpräsident
Mag. Dr. Rudolf GÜRTLER
em. Rechtsanwalt

Ehrenpräsident
Franz WIPFLI
Board Member, Zurich Financial Services

Ehrenpräsident
Dr. Arthur WULKAN
Partner, FIO Partners AG

DIREKTIONSRAT

Sandro ALBIN
Co-Founder, Managing Partner, cptr AG, Zürich

Michael BICKEL
CFO, Ivoclar Vivadent AG, Schaan

Gerhard BURTSCHER
Vorstands-vorsitzender, Bank für Tirol und Vorarlberg AG, Innsbruck

Frédérik DE BADRIHAYE
Repräsentant, Blanc Rouge AG, Vaduz

Dipl.-Ing. Christian DIEWALD
CEO, Stadler Austria GmbH, Wien

Hendrik FRECKEN MSc.
Senior Manager, Detecon Consulting Austria GmbH, Wien

Mag. Gerald GAHLEITNER
Steuerberater, Wirtschafts-prüfer, Partner LeitnerLeitner GmbH, Linz

Dr. Burkhard GANTENBEIN
Geschäftsführender Gesellschafter, Ango Invest GmbH, Wien

Thorsten HEILING
Geschäftsführer, Vitra Ges.m.b.H., Wien

Mag. Lukas HELD LL.M.
Partner, hba Rechtsanwälte GmbH, Graz

Sarah HUBER
Geschäftsführerin, Nestlé Österreich GmbH, Wien

Mag. Stefan KARGL
Geschäftsführer, LMM Investment Controlling AG, Wien

Daniel KNUCHEL lic. oec. HSG
Partner, Advicum Consulting GmbH, Wien

Mag. Claudia KOPETZKY
Chief Marketing Officer, Axess AG, Anif

Dr. Rudolf KRICKL
Senior Partner, PwC Österreich GmbH, Wien

Ali KULEIN
CEO, Lindt & Sprüngli (Austria) Ges.m.b.H., Wien

Dr. Robert LÖW
Vorstands-vorsitzender, Liechtensteinische Landesbank (Österreich) AG, Wien

Christian Paul LYK
CEO, KENDRIS AG, Zürich

Mag. (FH) Michael MOOSLEITHNER
Consultant, Zürich

Mag. Thomas NEUSIEDLER
CEO, Helvetia Versicherungen Österreich AG, Wien

Christoph OBERERLACHER, MBA
Geschäftsführer, Swiss Life Select Österreich GmbH, Wien

Dr. Claudio PASSARDI
CFO, Zürich Versicherungs AG Österreich, Wien

Mag. Sonja PEDROSS-AICHINGER
Geschäftsführerin, Bühler AG, Salzburg

Wolfgang ROSAM
Herausgeber Chefredakteur, Falstaff Verlags GmbH, Wien

Julien ROSSIER
Geschäftsführer, Bucherer 1888, Wien

Mag. Helmut SALLER
Geschäftsführer, The Swatch Group (Österreich) GmbH, Wien

Christian D. SCHÄFER
Vorstand, Laufen Austria AG, Wilhelmsburg an der Traisen

Mag. Helmut SCHOBA, MBA
Geschäftsführer, VGN Medien Holding GmbH, Wien

Roland SCHUBERT
Mitglied des Verwaltungsrats, LGT Bank AG, Vaduz

Janine SCHWABE-HÄDER
Vorsitzende der Geschäftsführung, Schindler Aufzüge und Fahrtreppen GmbH, Wien

Alessandro SERALVO
Executive Vice President, Cornèr Banca SA, Lugano

Rainer STEINLESBERGER
CEO Österreich, Zühlke Engineering AG, Wien

Dr. iur. Klaus TSCHÜTSCHER
Verwaltungsrat, Swiss Life Holding AG, Zürich

ADVISORS

Rudolf SEMRAD
Senior Advisor, HKSÖL, Wien

Yvonne FIEDERMANN
Advisor, HKSÖL, Zürich

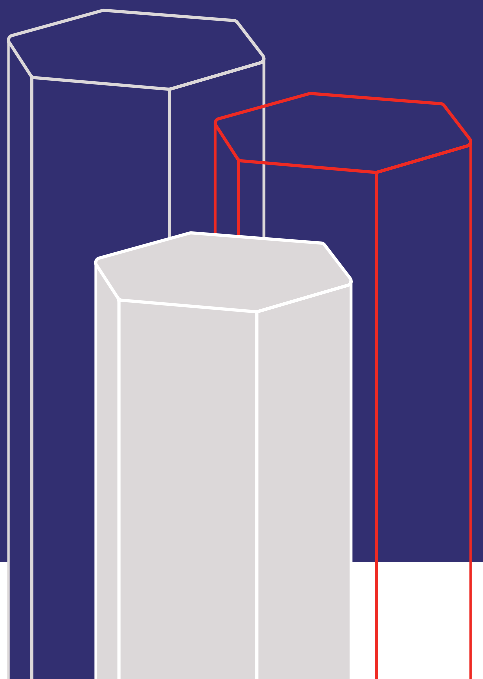
HANDELSKAMMER
Schweiz ■ Österreich ■ Liechtenstein

Gut für Sie.
Gut für Ihr Geschäft.

Mit dem Eintritt in die Handelskammer Schweiz-Österreich-Liechtenstein (HKSÖL) werden Sie Teil eines hochkarätigen Netzwerks von Führungskräften im Wirtschaftsraum Schweiz-Österreich-Liechtenstein.

Profitieren auch Sie von unseren Kontakten und zahlreichen Vorteilen und werden Sie Mitglied!

Jetzt beitreten!



Exklusive Vorteile
für unsere Mitglieder

Events
Veranstaltungen mit hochkarätigen Speakern und Raum zum Netzwerken.

Match-Making
Vernetzung mit gewünschten Zielpersonen durch den HKSÖL-Generalsekretär.

Meetings
Buchbarer Veranstaltungssaal in Wien und Räume bei Partnern in Zürich und Vaduz.

Versicherung
Kostenlose Unfall- und Rechtsschutzversicherung für zwei Angestellte Ihres Unternehmens.

Adressrecherche
Einmal im Jahr eine kostenlose Adressrecherche für Mitglieder.

Spezialraten
Corporate Rates bei ausgewählten Hotels und der People's Airline.

Mehrwertsteuerrückforderung
Unterstützung bei der Erstattung der bilateralen Mehrwertsteuer.

Dokumentenservice
Recherche und Unterstützung bei Bonitätsprüfungen, Handelsregisterauszügen u.v.m.

Team

Urs WEBER	Katharina SILVA GUERRERO	Martin KAISER	Selina SCHALKO	Nermin KURTIĆ
Generalsekretär	Marketing-management	Event-management	Projekt- und Mitglieder-management	Finanz-management

LinkedIn:
company/hk-schweiz

Blog:
hk-schweiz.at/blog

Kostenloses Hub-Abo:
hk-schweiz.at/abonnieren

Willkommen im Team

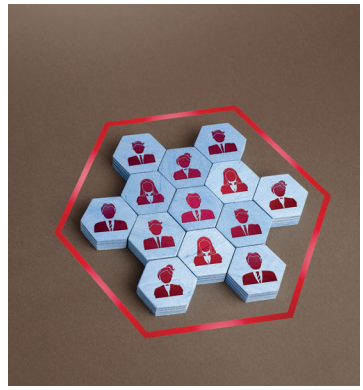
Wir freuen uns über Verstärkung: Mit Nermin Kurtić gewinnt unser HKSÖL-Team Unterstützung im Finanzmanagement.

Wirtschaft und Pflege sind für mich kein Widerspruch, sondern die Basis einer zukunftsfähigen Symbiose. Ich verbinde ökonomische Präzision mit sozialer Menschlichkeit. Während Zahlen die Sprache des Erfolgs sprechen, ist Empathie die Währung, die nachhaltiges Vertrauen schafft und langfristige Geschäftsbeziehungen lebendig hält.

Nermin Kurtić

Seit März 2026 unterstützt Nermin Kurtić unser HKSÖL-Team im Finanzmanagement. Er bringt fundierte Praxiserfahrung aus seiner vorherigen Tätigkeit bei Sabo + Mandl & Tomaschek Immobilien GmbH mit, wo er als Immobilienbuchhalter und Personalverrechner die finanzielle Verantwortung für das Hausbetreuungspersonal innehatte. Neben seiner geringfügigen Anstellung bei der HKSÖL schlägt Herr Kurtić eine Brücke zwischen zwei Welten: Durch sein duales Studium der Wirtschaftsberatung an der Fachhochschule Wiener Neustadt und der Gesundheits- und Krankenpflege an der Hochschule Campus Wien verbindet er analytisches Denken mit tiefem sozialem Verständnis.

Wir freuen uns, mit ihm eine engagierte und kompetente Persönlichkeit für unser Team gewonnen zu haben!



NEUE HKSÖL-MITGLIEDER

Frontview Advisory Group AG
Strategie- und Organisationsberatung
CH-8712 Stäfa
frontviewadvisory.com

Gensch Personal GmbH
Personalvermittlung und Personaldienstleister für Zeitarbeit
AT-1010 Wien
gensch.at

Madis Consulting Kft.
Software-Dienstleistungsunternehmen
HU-1133 Budapest
madis.hu

DINKO (13) Beteiligungsverwaltung und Management GmbH
Beteiligungsentwicklung und Beratung
AT-1130 Wien

Kyndryl Switzerland GmbH
Anbieter von IT-Infrastrukturdiensten
CH-8005 Zürich
kyndryl.com

TRIFOLIUM PARTNERS
Vermögensberatung
AT-2540 Bad Vöslau
trifolium-partners.com

Reitbauer & Experts
Tourismusberatung
AT-1180 Wien
reitbauerandexperts.com

Mehr Infos zu den neuen Mitgliedern finden Sie hier:

Mehrwertsteuer-Rückforderung

Österreichische Unternehmer, die in der Schweiz bzw. Liechtenstein weder ihren Sitz noch eine Betriebsstätte haben, können unter bestimmten Voraussetzungen ihre Mehrwertsteuer geltend machen. Dasselbe gilt für Schweizer bzw. liechtensteinische Unternehmen in Österreich.

Wichtig für die Mehrwertsteuer-Rückerstattung ist, dass der Antragsteller im eigenen Land steuerpflichtig ist.

Rückerstattet wird die MwSt beispielsweise für **Hotel-, Reise- oder Veranstaltungskosten**.

Anerkannt werden ausschließlich Originalrechnungen, ausgestellt auf das Unternehmen, bei denen die Vorschriften über die Ausstellung von Rechnungen und die Voraussetzung für den Vorsteuerabzug erfüllt sind.

VORAUSSETZUNG IST, DASS DER UNTERNEHMER

- keine Umsätze im Antragsland erzielt oder
- nur steuerfreie Güter-/Personenbeförderungen mit Schiffen oder Luftfahrzeugen ausführt oder
- nur Umsätze ausführt, für welche die Steuerschuld auf den Leistungsempfänger übergeht (Reverse-Charge) oder
- nur elektronische Dienstleistungen vom Drittland aus an Nichtunternehmer erbringt und von der Sonderregelung des § 25a UStG 1994 bzw. Art. 26 c der 6. EG-Richtlinie Gebrauch gemacht hat.

Deadline ist der 15. Juni des Folgejahres. Die Antragstellung für eine 2025 bezahlte Mehrwertsteuer muss bis **spätestens 15. Juni 2026** erfolgen.

Wir unterstützen Sie bei der Prüfung der Voraussetzungen, der Abklärung der Steuerschuld und bei der Einreichung.

Kontakt:
Katharina Silva Guerrero M.A.
silva@hk-schweiz.at
+43 1 512 59 59 77

Weitere Informationen und Antragsformulare finden Sie auf hk-schweiz.at/leistungen

Hier scannen!


People's
EXPERIENCE THE DIFFERENCE
Perfekte Tagesrand-zeiten
WIEN & BODENSEEREGION
Fliegen Sie mit der Fluglinie People's bequem und stressfrei in nur 60 Minuten von Wien in die Bodenseeregion oder von St. Gallen-Altenrhein in die Bundes-hauptstadt – wochentags mit jeweils zwei Flügen pro Tag.
for people. by people.