

# Sicherheit im Wandel

Die Konferenz „Future-Hub: Sicherheit“ widmete sich den Herausforderungen in einer Zeit multipler Krisen und neuer technologischer Entwicklungen.

**K**riege in der Ukraine und im Nahen Osten, Fake News und Cyber-Kriminalität erzeugen Verunsicherung in der Gesellschaft, das Thema Sicherheit gewinnt an Bedeutung. Mit der Konferenz „Future-Hub: Sicherheit“ griff die *imh GmbH*, Veranstalter von Fachkonferenzen, eine der Herausforderungen der Gegenwart auf. Die Veranstaltung mit über hundert Besuchern fand am 2. Dezember 2025 im *Impact Hub Vienna* statt. Hochkarätige Referenten beleuchteten, wie Sicherheit unter den Bedingungen geopolitischer und technologischer Veränderungen gewährleistet werden kann.

Franz Ruf, Generaldirektor für die öffentliche Sicherheit im Bundesministerium für Inneres, sprach über physische und digitale Sicherheit. „Externe Konfliktlagen werden zu nationalen Bedrohungen“, sagte Ruf. Der Nahostkonflikt wirkt in unsere Gesellschaft hinein, schürt die Polarisierung und erhöht die Terrorismusgefahr. In den letzten Jahren konnten mehr als zehn Terroranschläge, etwa auf die geplanten Taylor-Swift-Konzerte und den Stephansdom, verhindert werden. Im November 2025 wurde ein Waffenlager eines mit der Terrororganisation Hamas in Verbindung stehenden Netzwerks ausgehoben. Die Waffen waren für Anschläge in Österreich oder anderen EU-Ländern gedacht.

**Sicherheitskonzept.** Ruf nannte drei Punkte, die für ein zeitgemäßes Konzept der Sicherheit essenziell sind: 1. Physische und digitale Sicherheit sind nicht mehr voneinander trennbar, IT-Sicherheit und Objektschutz dürfen deshalb nicht isoliert betrachtet werden. 2. Digitale Technologien und künstliche Intelligenz werden einerseits von Kriminellen genutzt, etwa zur Desinformation oder für Phishing-Attacken. Die Polizei muss deshalb in die Lage versetzt werden das auch zu tun: für Analyse, Prognosen und forensische Auswertung. 3. Im Bereich der Sicherheit ist eine der wichtigsten Ressourcen Vertrauen. Dieses kann durch klare Kommunikation und Transparenz vor, während und nach einer Krise gestärkt werden.



„Future-Hub: Sicherheit“: Expertinnen und Experten beleuchteten, wie Sicherheit unter den Bedingungen geopolitischer und technologischer Veränderungen gewährleistet werden kann

**Neue Weltordnung.** Peter Vorhofer, nationaler Sicherheitsberater im Bundeskanzleramt, stellte die Frage „Wie sicher ist Österreich wirklich?“ und beantwortete diese, indem er die Lage in Österreich im Kontext der globalen internationalen Beziehungen betrachtete. Diese haben sich in den letzten Jahren verändert. Die bipolare Weltordnung existiert in dieser Form nicht mehr, in Zukunft werden weitere Machtzentren wie China, Indien oder Brasilien, dazukommen.

Vorhofer strich die Wichtigkeit der geistigen Landesverteidigung, insbesondere in Zusammenhang mit hybriden Bedrohungen, heraus: „Polizei, Streitkräfte und Blaulichtorganisationen produzieren Sicherheit. Wir brauchen aber auch die Bevölkerung, damit wir alle Bedrohungen abwehren können, etwa die subtile Beeinflussung der Meinung.“

**Polizei-Drohnen.** Einen zunehmend wichtigeren Beitrag zur Aufrechterhaltung der öffentlichen Sicherheit leisten Drohnen. Chefinspektor Wolfgang Schwarz von der Direktion Spezialeinheiten/Einsatzkommando Cobra bot in

seinem Vortrag einen Überblick über Einsatzmöglichkeiten von Drohnen bei der Polizei. Derzeit gibt es bei der österreichischen Polizei über 600 Drohnenpiloten. Die Drohnen sind mit optischen Kameras, Wärmebildkameras, zum Teil auch mit Systemen zur Bild- und Datenanalyse oder mit Lautsprechern für Durchsagen ausgestattet.

Bei Großveranstaltungen wie dem Donauinselfest, Fußball-Risikospielen und großen Kundgebungen liefern Drohnen den Einsatzkräften einen Gesamtüberblick. Weitere Einsatzbereiche sind Observationen, Brandermittlungen, Objektschutz, Grenzüberwachung und die Überwachung der kritischen Infrastruktur. Drohnenpiloten unterstützen bei Personenfahndungen, bei der Suche nach abgängigen Personen sowie im Bereich der Verkehrspolizei – dank der Zoom-Funktion der Drohnenkameras kann man ein Kfz-Kennzeichen aus eineinhalb Kilometern Entfernung auslesen.

**Unternehmenssicherheit.** Eine Reihe von Vorträgen befasste sich mit Sicherheit aus der Perspektive der Wirtschaft. Dabei wurde deutlich, dass der

Schutz vor Cyber-Angriffen zu den größten sicherheitsrelevanten Herausforderungen für Unternehmen zählt. Häufig ist die IT-Infrastruktur veraltet und nicht ausreichend vor Angriffen geschützt.

Für Christian Paul, Leiter der Abteilung Konzernsicherheit & Resilienz der *Österreichischen Post AG* und ehemaliger Polizeibeamter, stellt menschliches Fehlverhalten das größte IT-Sicherheitsrisiko dar, etwa durch unvorsichtigen Umgang mit sozialen Medien.

Zur Stärkung der Cyber-Sicherheit innerhalb der Europäischen Union wurde 2023 die NIS-2-Richtlinie verabschiedet, die die NIS-Richtlinie aus 2016 ersetzt und den Anwendungsbereich auf einen größeren Teil der Wirtschaft erweitert.

In Österreich erfolgt die Umsetzung durch das Netz- und Informationssystemsystemsicherheitsgesetz (NISG), das im Oktober 2026 in Kraft treten wird. Es verpflichtet Unternehmen, die Wirksamkeit ihrer Schutzmaßnahmen regelmäßig zu prüfen und ihre Mitarbeiter durch Schulungen für Cyber-Risiken zu sensibilisieren.



**Konferenz „Future-Hub: Sicherheit“:**  
**Franz Ruf, BMI, Peter Vorhofer, Bundeskanzleramt, Christian Paul, Post AG, Wolfgang Schwarz, BMI**

**Künstliche Intelligenz.** In drei zur Auswahl stehenden Sessions – digitale Sicherheit, Arbeitsschutz und Sicherheitskultur – konnten sich die Konferenzteilnehmer mit jeweils einem sicherheitsrelevanten Themen vertieft auseinandersetzen. In der Session zu digitaler Sicherheit legte Andreas Gruber, Geschäftsführer der KI-Prüf- und Zertifizierungsstelle *TRUSTIFAI*

*GmbH*, den Schwerpunkt auf künstliche Intelligenz. Mit dem AI Act hat die Union erstmals EU-weit verbindliche Regeln für den Einsatz von KI geschaffen, die schrittweise ab 2026 bzw. 2027 anzuwenden sind.

Je höher das potenzielle Risiko eines KI-Systems ist, desto strenger fallen die Anforderungen an Entwicklung, Einsatz und Kontrolle aus. Als Grundlage für den AI Act dienen internationale Normen wie die CEN/CENELEC-Richtlinien und ISO-Standards, die vorschreiben, dass Risiken systematisch identifiziert, bewertet und behandelt werden müssen.

Bei der Verwendung von KI können Verzerrungen in den Daten (Bias) auftreten, die in der Folge diskriminierende Entscheidungen begünstigen. Ein weiteres Problem besteht darin, dass alle KI-Systeme menschliche Aufsicht benötigen. Da Menschen nur über eine begrenzte Aufmerksamkeitsspanne verfügen, muss auch ihre Fehleranfälligkeit Teil der Risikoanalyse sein. Grundsätzlich gilt laut Gruber, dass KI nur dort eingesetzt werden sollte, wo es sinnvoll und notwendig ist.

*Rosemarie Pexa*