Kybernet-Pass (K-PASS)

Sicherheitsforschung made in Austria als Beitrag zur europäischen Cyberresilienz

Präsentation bei ICIRCLE am 24.11.2025

Autoren: Dr. Ralph Hammer / Adrian Koch
Stabsstelle f. Sicherheitsforschung und Technologietransfer Wien, 18.11.2025

Sicherheitsklammer – Drei Programme

KIRAS
Sicherheitsforschung

K-PASS

FORTE
arma et scientia
ex officio

Grundlegendes

- **KIRAS, FORTE** und **Kybernet-Pass** (K-PASS) bilden gemeinsam die **„Österreichische Sicherheitsklammer“**
- **Ziel von Kybernet-Pass**: Unterstützung bei der **Entwicklung neuer Technologien** und der Schaffung des erforderlichen Wissens, um **Sicherheit Österreichs** zu erhöhen und heimische **Wertschöpfung** zu generieren
- Durch staatliche Beihilfe sollen **marktnahe Forschungsergebnisse** für entsprechende **Sicherheitsanwender** (Blaulichtorganisationen, Militär, Betreiber krit. Infrastrukturen) geschaffen werden

Kybernet-Pass
K-PASS

Programmname als **Porte-Manteau** (Kofferwort), setzt sich zusammen aus

- **„Kybernetik“ statt „Cyber“,** um die Notwendigkeit einer nationalen Forschungsförderinitiative für digitale Sicherheit zu unterstreichen
- **„Pass“** steht für die erfolgreiche Umsetzung iSv „to pass“ und spielt dabei an auf
- den **Khyber-Pass in Afghanistan**, dessen Kontrolle zentral für den Waren-, Truppen- und Wissensverkehr des Britischen Empires von und nach Indien war, als Allegorie darauf, dass Wohlstand und Bewegungsfreiheit auch digital nur möglich sind, wenn man die „unangenehmen“ strategischen Pflichten der notwendigen Sicherheit erfüllt.

Umsetzung

- Kybernet-Pass basiert auf **Verwaltungsübereinkommen zur digitalen Sicherheitsforschung zwischen BMF und BKA** vom 22. Dezember 2022
- **BMF** besitzt **Programmeigentümerschaft** (Finanzierung und Organisation), **BKA** koordiniert **sicherheitspolitischen Forschungsbedarf** (inhaltlich / thematische Ausgestaltung)
- **Strategische Koordination** im Rahmen des erweiterten **Lenkungsausschusses** für das österreichische Sicherheitsforschungsprogramm KIRAS
- **Programm-Management** übernimmt die **FFG**

Spezifika

- **Forschungsfokus:** Digitale Sicherheitsthemen inkl. dual-use, die von verschiedenen Bedarfsträgern eingebracht werden.
- Ein erfolgreiches Kybernet-Pass-**Konsortium** für ein Projekt muss sich zumindest aus je einem **Bedarfsträger, Forscher, Unternehmen** und **GSK-Experten** zusammensetzen
- Förderung von **nicht-österreichischen Teilnehmern** ist bei Kybernet-Pass möglich (bis max. 20% der Gesamtprojektkosten)

Themen

- Sicherheit von „security“-relevanter Soft- und Hardware
- Schutz für IoT-Anwendungen und Netze
- Cyber Crime und Digitale Forensik
- E-Government-Schutz (inkl. Aufrechterhaltung des Vertrauens in der Bevölkerung)
- Steganografie und digitale Datenanalyse (Post-Quantenverschlüsselung)
- Der User als Teil der digitalen Dimension (Datensicherheit, Cyber-Stalking, Cyber-Mobbing)
- Sicherheit & Künstliche Intelligenz
- Hybride Bedrohungen (inkl. Deep fake-Erkennung)
- Schutz für IKT-Systeme als „smarte“ kritische Infrastruktursysteme (z.B. autonome Mobilität, smarte Strom- und sonstige Versorgungsnetze) inkl. Resilienz, Versorgungssicherheit und Vertrauensüberprüfung (vor allem Themen für Breitbandausbau und 5G-Netze)

Zahlen und Daten

- BMF plant mit einem **jährlichen** Kybernet-Pass-**Ausschreibungsbudget von € 5 Mio.**

- Bei den Ausschreibungen sollen **verschiedene FFG-Förderinstrumente** zur Anwendung kommen, darunter solche mit **Förderraten bis zu 85%** (Ausnahme Instrument F&E-DL: Finanzierung 100%)

- Die **Sicherheitsklammer** verfügt damit über ein **Gesamtbudget von € 16 Mio. f. 2025**, das mit € 6 Mio. f. KIRAS, € 5 Mio. f. FORTE und € 5 Mio. f. Kybernet-Pass aufgeteilt wird

- Bisher wurden in K-PASS **24 Projekte mit € 12,6 Mio**. (Sikla gesamt: 558 Projekte mit rd. € 209 Mio.) gefördert.

KIRAS/K-PASS-Projekte zur Cybersicherheit von Unternehmen*

- **CONTAIN –** Effiziente Reaktion auf IT-Sicherheitsvorfälle in transnationalen Lieferketten
- **CyberGuide** - Entwicklung eines Leitfadens für österreichische KMU zur Verbesserung ihrer Cybersicherheit
- **CyberTASTE** – Cyber Range Technology Stack and Simulations for Training and Evaluation
- **CyberMonoLog –** Cyber Security MONITORING and LOGGING Best Practice Guidance
- **Fake-Shop-Detecto**r – Tool entwickelt aus Projekten SINBAD (Sicherheit vor organisiertem Internet-Bestellbetrug) und RIO (Resilienz im Online-Handel)
- **GENESIS –** Guideline für Behörden und KMU-Anbieter strategischer Services zur risiko-orientierten Implementierung der NIS-Richtlinie
- **ACCSA** – Austrian Cyber Crises Support Activities
- **Cloud Sicherheit –** Leitfaden für Behörden und KMUs zur sicheren Cloud Nutzung
- **ATLAWS** – Atlas for Tracking Law And Watching Standards (Ko-Finanzierung durch BMF) umgesetzt durch RESEARCH INSTITUTE AG & CO KG

* Weiterführende Informationen finden sich unter http://www.kiras.at/gefoerderte-projekte

Innovation – Was nun?

- Nach TRL 6 (Prototyp/Demonstrator) gibt es starken Abfall der staatlichen Förderintensität bis zu TRL 9 (Markteinführung) → „Tal des Todes“ f. Innovationen

- Zur Verh(m)inderung des „Tal des Todes-“Effekts für Innovationen zwischen TRL 6 und TRL 9 (Markteinführung) haben BMF und FFG seit 2023 das Instrument Innovation AKUT eingeführt (basiert auf F&E-DL, daher Finanzierung 100%!)

- Innovation AKUT finanziert den Einsatz von Prototypen/Demonstratoren bei Bedarfsträgern (Mindest-Konsortialstruktur: 1 Bedarfsträger und 1 AT-Unternehmen) für max. 1 Jahr mit max. € 100 k

- Innovation AKUT wird zumindest dreimal jährlich ausgeschrieben und verfügt über ein verkürztes Bewertungsverfahren zur Wirkungsoptimierung des Instruments

Sicherheitsforschungslandkarte KIRAS

Die Sicherheitsforschungslandkarte KIRAS wurde im Dezember 2009 vom bmvit eingerichtet mit dem Ziel:

- Anwender (= Bedarfsträger wie Bundesministerien, Landesbehörden, Blaulichtorganisationen, Betreiber kritischer Infrastrukturen);
- Forscher;
- Unternehmen;
- Geistes-, Sozial und Kulturwissenschaftler;

auf dieser Internetplattform ihren Bedarf sowie ihre Fähigkeiten darstellen zu lassen und so die Schaffung von Konsortien für KIRAS-Projekte dank einfacher Bedienung zu erleichtern. Bisher haben über 500 Institutionen diese kostenlose Möglichkeit der Repräsentation wahrgenommen.

http://landkarte.kiras.at/

KIRAS- Call 2025/26 offen

Ausschreibungsdauer: 06.Oktober 2025 – 06.März 2026 (Inno AKUT: 30.01.2026)
Unterlagen & E-Call: KIRAS/K-PASS 2025 | FFG

Sicherheitsforschung – Und was geschieht in Europa?

- Österreichische Teilnehmer sind an jedem 3. geförderten EU-Sicherheitsforschungsprojekt beteiligt. Die österreichische Rückflussquote beträgt bei einem österreichischem Budgetbeitrag von 2,5% (durchschnittlicher Rückfluss AT: 2,9%) klar überdurchschnittliche 3,9%!

- Im aktuellen 9. EU-Forschungsrahmenprogramm „Horizon Europe“ stehen im Cluster 3, „Civil Security for Society“ (2021-2027), rd. € 1,6 Mrd. (davon rd. € 500 Mio. f. Cybersicherheit) zu Verfügung

- Aktuell wird das Europäische Kompetenzzentrum für Cybersicherheit (ECCC) in Bukarest eingerichtet, das die Cybersicherheitsforschung in den EU-Förderprogrammen „Digital Europe“ und für „Horizon Europe“ (aktuell nur bei Ko-Finanzierungen!!) koordinieren soll

Erkenntnisse zum Thema Cyberkriminalität und Unternehmen

- Im „Wettrüsten zwischen Cyberangriff und –abwehr haben **die Kriminellen die Initiative → KI als Game-Changer?**
- Kosten-Leistungsverhältnis begünstigt aktuell ebenfalls den Angreifer
- **Forschung hilft,** die technische wie soziologische Abwehr zu stärken, kann aber Kosten-Leistungsverhältnis nicht ändern **→ Sicherheit kostet mehr als Angriff**
- **Abwehrkonzepte sind grundsätzlich passiv,** dem gescheiterten Angreifer drohen kaum eigene Konsequenzen **→ offensive Konzepte stärken**
- Der Staat kann seine Subjekte im digitalen Raum kaum wirksam schützen **→ die digitale Welt kennt keine Ordnung** („Im Cyberwald, wo die Digi-Räuber hausen")
- **Fazit:** Die digitale Wirtschaft lebt und wirkt in einer virtuellen „Vormoderne" **→ wirksames Mittel** seit der Antike **zur Schadensbegrenzung sind aktuell Versicherungen** (digitales „Seedarlehen")

Danke für Ihre Aufmerksamkeit!

Ansprechpartner BMF:
Dr. Ralph HAMMER
Stabsstelle f. Sicherheitsforschung und Technologietransfer
Sektion VI, BMF, Wien
ralph.hammer@bmf.gv.at

Informationen zu Programm und Projekten:
www.kiras.at

Ansprechpartner FFG:
DI Sabine KREMNITZER f. KIRAS und FORTE
Sabine.kremnitzer@ffg.at

Dr. Polina WILHELM f. Kybernet-Pass
polina.wilhelm@ffg.at

DI Jeannette KLONK f. EU-Sicherheitsforschung
jeannette.klonk@ffg.at