FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

SiKu-KRITIS

Sicherheitskultur in der Kritischen Infrastruktur

Forschungsprojekt – Kurzbericht

VERWALTUNG, WIRTSCHAFT, SICHERHEIT, POLITIK

Bundesministerium Finanzen

FFG Forschung wirkt.

KIRAS Sicherheitsforschung

Sicherheitskultur als Basis für Resilienz in Unternehmen

Fotostudio Huger

Dr. Reinhard Marak
Leiter Stabstelle Krisenmanagement und Sicherheitsvorsorge der WKÖ

Der Schutz Kritischer Infrastrukturen ist seit einem Jahrzehnt ein wesentlicher Aspekt für die Aufrechterhaltung der (Versorgungs-)Sicherheit in Österreich. Nicht zuletzt mit der nationalen Umsetzung der RKE-Richtlinie entwickelt sich das Schutzziel von vorrangig sicherheitspolizeilichen Überlegungen hin zu einem umfassenderen Schutz, der auch die Resilienz von betrieblichen Abläufen und Produktion im Unternehmen sowie Schulungsmaßnahmen von Beschäftigten einschließt.

Für die betroffenen Unternehmen resultieren aus den RKE-Regularien hilfreiche Unterstützungen durch die Sicherheitsbehörden, aber auch Verpflichtungen und zum Teil erhebliche Investitionen in Sicherheitsmaßnahmen.

Eine Basis für die innerbetriebliche Sicherheit und damit für die Resilienz im Unternehmen bildet das Verhalten und die Interaktion von Beschäftigen mit Besucherinnen und Besuchern im Unternehmen. Solche „weichen" Maßnahmen waren bislang kaum im Fokus der Sicherheitsforschung. Von diesen Themen hängt aber auch ab, wie beispielsweise der Schutz von kritischen Informationen im Alltag gelebt wird und in welchem Ausmaß die Beschäftigten vor Bedrohungen und Übergriffen durch externe Personen geschützt werden.

Mit dem Projekt SiKu KRITIS werden solche unternehmensinternen Sicherheitsaspekte wissenschaftlich untersucht und Empfehlungen abgeleitet. Es zielt dabei auf Unternehmen und Einrichtungen der Kritischen Infrastruktur ab. Die Ergebnisse zur Bewertung und Verbesserung der innerbetrieblichen Sicherheitskultur können und sollen auch für andere Unternehmen, insbesondere wenn sie eine hohe Systemrelevanz haben, nutzbar gemacht werden. Damit kann die Versorgungssicherheit in Österreich verbessert werden.

Impressum
Medieninhaberin: FH Campus Wien – Verein zur Förderung des Fachhochschul-, Entwicklungs- und Forschungszentrums im Süden Wiens; ZVR-Zahl 625976320, Favoritenstraße 226, 1100 Wien.
Für den Inhalt verantwortlich: FH-Prof.in Mag.a Claudia Körmer; FH-Prof. DI Dr. Martin Langer.
Projektsupport: Mirjam Johanna Habisreutinger, MA; Kristina Hauer, BA.
Redaktionelle Aufbereitung: DI (FH) Mag. Thomas Goiser MBA MA.
Lektorat: Mag.a Verena Brinda, www.verenabrinda.at.
Grafik: Doris Zemann, www.dggd.at; Druck: Berger Horn
Die Texte und Daten wurden sorgfältig ausgearbeitet; dennoch können wir keine Haftung für die Richtigkeit der Angaben übernehmen.

Inhaltlicher Redaktionsschluss: 15. Juli 2024.

Kontakt für Feedback: risikomanagement@fh-campuswien.ac.at
Wien, im September 2024
https://doi.org/10.34895/fhcw.0019

Das Projekt SiKu KRITIS wird gefördert im Rahmen des Programms KIRAS durch das Bundesministerium für Finanzen und von der Österreichischen Forschungsförderungsgesellschaft abgewickelt. (www.kiras.at)

Forschung und Entwicklung, die der Gesellschaft dient

FH Campus Wien/Schedl

FH-Prof.in Mag.a Dr.in Elisabeth Haslinger-Baumann, DGKP
Vizerektorin für Forschung und Entwicklung an der FH Campus Wien

Die FH Campus Wien ist mit über 8.000 Studentinnen und Studenten in nahezu 70 Studiengängen sowie zehn fachspezifischen Forschungszentren Österreichs größte Fachhochschule. Interdisziplinarität und anwendungsorientierte Forschung und Entwicklung sind unsere Mission – zum Nutzen unserer Projektpartnerinnen und Projektpartner sowie zum Wohle der Gesellschaft. Unseren Erfolg als Fachhochschule haben wir unseren Forschenden und Lehrenden zu verdanken. Sie sind unsere wertvollste Ressource.

Allein im Geschäftsjahr 2022/23 konnten wir mit unseren Forschungsprojekten einen Auftragsstand von insgesamt 12 Millionen Euro und einen Umsatz von 4,2 Millionen Euro erzielen. Das wird in diesem Zeitraum mittels 97 drittmittelfinanzierten Projekten erreicht. Diese erfreuliche Bilanz kann voraussichtlich im heurigen Budgetjahr noch übertroffen werden.

In unseren Forschungsprojekten kooperieren wir mit anderen Hochschulen, dem öffentlichen Sektor, dem Sozial- und Gesundheitssektor und zahlreichen Unternehmen – vom KMU bis zur Industrie – und bewegen uns in nationalen und internationalen Netzwerken.

Das KIRAS-Projekt „Konzeptualisierung und Erhebung der Sicherheitskultur in der Kritischen Infrastruktur (SiKu KRITIS)“ ist ein ganz besonderes Projekt. Es wird von einem Expertinnen- und Experten-Team des Fachbereichs Risiko- und Sicherheitsmanagement geleitet und ist ein Paradebeispiel eines erfolgreichen interdisziplinären Teamplays: Mit der Wirtschaftskammer Österreich, der Johannes Kepler Universität Linz, der Austrian Power Grid, dem Wiener Gesundheitsverbund und den Österreichischen Bundesbahnen sind starke Partnerinnen und Partner an Bord, die ihre jeweilige Expertise einbringen, um den Umgang mit dem Schwerpunkt „Sicherheit“ in Kritischen Infrastrukturen zu analysieren.

Die Sicherheitskultur in Organisationen wurde in Österreich bisher hauptsächlich im Zusammenhang mit Unfällen erforscht. Das Konsortium hinter SiKu KRITIS stellt jetzt Angriffe auf Unternehmen wie Wirtschafts- und Industriespionage, Cyberangriffe oder Übergriffe auf Mitarbeiterinnen und Mitarbeiter in den Fokus der Sicherheitsbewertung. Forschungsziele sind dabei unter anderem eine Konzeptualisierung des Begriffs „Security Culture“, die Analyse des Status Quo der Security Culture am Beispiel von drei Organisationen aus den Bereichen Gesundheit, Verkehr und Mobilität sowie Energie und die daraus abgeleiteten Empfehlungen für eine Verbesserung der Security Culture in diesen Organisationen.

SiKu KRITIS zeigt: Sicherheit braucht Qualitätsstandards, Kooperation und einen gesamtheitlichen Blick. Es gibt spannende Forschungsergebnisse und einen konkreten Nutzen, den diese für das gesellschaftliche Miteinander entfalten. Die Gesellschaft im Mittelpunkt – dafür steht die FH Campus Wien.

INHALTSVERZEICHNIS

SiKu KRITIS – Sicherheitskultur in der Kritischen Infrastruktur

Das KIRAS-Projekt SiKu KRITIS wurde unter der Leitung der FH Campus Wien in der geplanten Projektlaufzeit von November 2022 bis November 2024 umgesetzt. SiKu KRITIS beschäftigte sich mit der Konzeptualisierung und Erhebung der „Security Culture“ in drei ausgewählten Organisationen der KRITIS in Österreich.

Als Hauptbedarfsträger fungierte dabei die Wirtschaftskammer Österreich (WKÖ) – Stabstelle Krisenmanagement und Sicherheitsvorsorge. Darüber hinaus waren die Johannes Kepler Universität Linz (JKU), die Austrian Power Grid AG (APG), die Österreichischen Bundesbahnen (ÖBB) und der Wiener Gesundheitsverbund (WIGEV) Kooperationspartner. Zudem waren folgende Organisationen Teil des erweiterten Projektkonsortiums: Bundesministerium für Inneres (BMI), Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK), Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK), Österreichischer Rundfunk (ORF) und A1 Telekom Austria AG.

Sicherheitskultur in Organisationen wurde bisher hauptsächlich in Zusammenhang mit Unfällen erforscht. Wie aber die aktuellen Krisen zeigen, sind unter anderem intentionale Gefahren (wie Wirtschafts- und Industriespionage, Cyberangriffe, Diebstähle, Vandalismus und Übergriffe auf Beschäftigte) zunehmende Bedrohungen für Organisationen der KRITIS.

In den vergangenen zehn Jahren wurden einige wenige Ansätze zur Messung des Begriffs Security Culture (in Unterscheidung zu Safety Culture) entwickelt. Bisher existierte aber kein Ansatz, der eine wissenschaftliche Konzeptualisierung von Security Culture bietet, die als Basis für empirische Forschung geeignet wäre und relevante kriminologische Perspektiven inkludiert. Security Culture konnte dadurch bis dato nicht wissenschaftlich erfasst und gestaltet werden.

Der theoretische Fokus des Projekts lag daher auf einer umfassenden empirisch relevanten Konzeptualisierung von Security Culture. Diese wurde durch Sicherheitsverantwortliche im Hinblick auf ihre praktische Relevanz validiert. Im empirischen Teil wurde die Security Culture in Organisationen der KRITIS mit dem Fokus auf intentionale Gefahren erstmalig erhoben und analysiert. Davon umfasst war die Erforschung der Compliance der Mitarbeiterinnen und Mitarbeiter bezogen auf innerbetriebliche Sicherheitsnormen und die Erklärung von etwaigen Verstößen.

Jeweils ein Unternehmen aus den KRITIS-Sektoren Energie (APG), Mobilität (ÖBB) und Gesundheit (WIGEV) sollte mittels einem im Projekt entwickelten Mixed-Method-Ansatz aus qualitativen Befragungen und Analysen von sicherheitsrelevanter Infrastruktur und Dokumenten sowie quantitativem Fragebogen für Beschäftigte untersucht werden. Dies gelang bei den drei teilnehmenden Organisationen aus internen Gründen in unterschiedlichem Ausmaß – umfassend bei der APG, in etwas geringerem Ausmaß bei den ÖBB und beim WIGEV. Letzterer wurde mittels qualitativer Interviews und einer Dokumentenanalyse erforscht. Jede Organisation erhielt als Ergebnis einen vertraulichen Unternehmensbericht.

Im Rahmen eines Workshops mit Sicherheitsverantwortlichen aus verschiedenen Sektoren der KRITIS wurden die aus den Erhebungen gewonnenen Erkenntnisse diskutiert und allgemeine Empfehlungen zur Verbesserung der Security Culture entwickelt.

Der Abschlussbericht des Projekts enthält somit zusammenfassende Erkenntnisse aus den quantitativen und qualitativen Erhebungen der drei Partnerorganisationen sowie generelle Empfehlungen zur Verbesserung der Security Culture in der KRITIS.

SiKu KRITIS – Security Culture in Critical Infrastructure

SiKu KRITIS, a KIRAS project, was implemented within the planned project period from November 2022 to November 2024 under the direction of the University of Applied Sciences FH Campus Wien. It is dedicated to conceptualising and investigating the security culture of three selected organisations that are part of the critical infrastructure in Austria.

The Department for Crisis Response and Resilience of the Austrian Economic Chamber (WKÖ) was the main project partner. Cooperation partners were Johannes Kepler University Linz (JKU), Austrian Power Grid AG (APG), the Austrian Federal Railways (ÖBB) and the Vienna Hospital Association (Wiener Gesundheitsverbund, WIGEV). The following organisations were part of the project consortium: the Federal Ministry of the Interior (BMI), the Federal Ministry of Social Affairs, Health, Care and Consumer Protection (BMSGPK), the Federal Ministry for Climate Action, Environment, Energy, Mobility, Innovation and Technology (BMK), the Austrian Broadcasting Corporation (ORF) and A1 Telekom Austria AG.

Previously, research has focused on safety culture in connection with accidents at work. Current crises, however, clearly illustrate that intentional hazards such as economic and industrial espionage, cyber-attacks, theft, vandalism, and assaults on staff increasingly constitute a threat for critical infrastructure organisations.
In the last decade, different approaches were developed to enable the measurement of security culture, which is to be differentiated from safety culture. So far, no approach has provided a scientific concept of security culture that provides a basis for empirical research and considers pertinent criminological perspectives resulting in an inability to scientifically assess security culture or implement scientific findings in its organisation.
Hence, a comprehensive, empirically relevant conceptualisation of security culture formed the theoretical focus of the project, which was then validated by security officers in view of its practical relevance. In the empirical part of the project, we collected data on the security culture in critical infrastructure organisations, emphasising and analysing intentional hazards. This novel approach also included an analysis of the staff's compliance with internal security standards and explanations for any cases of non-compliance.

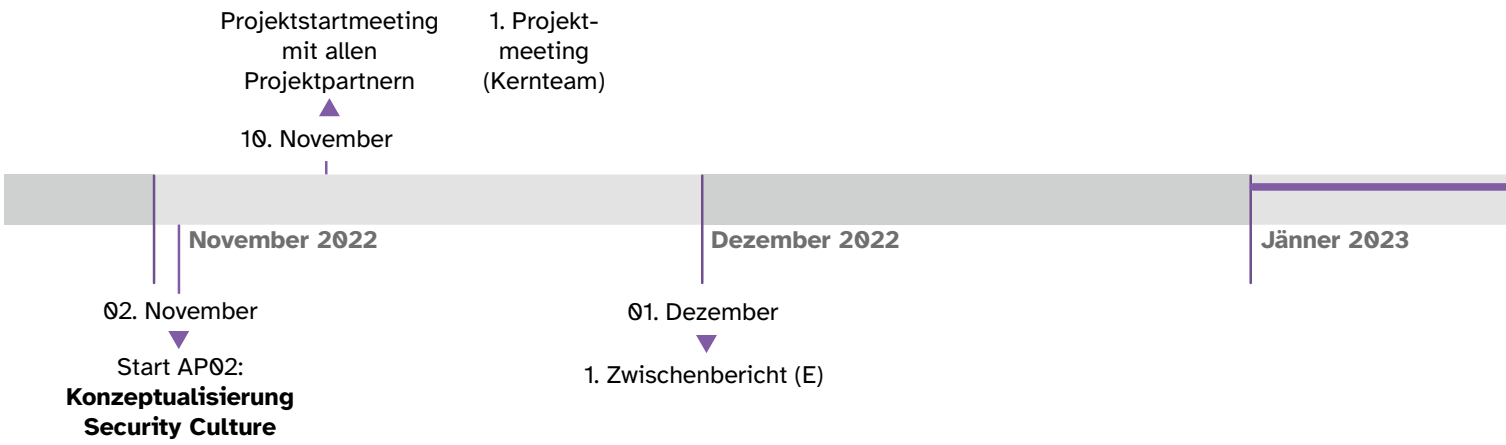
The project intended to analyse one organisation from each of the three critical infrastructure sectors energy (APG), mobility (ÖBB) and health (WIGEV), using a mixed-method approach. Developed as part of the project, it included qualitative surveys, an assessment of security-relevant infrastructure and documents as well as a quantitative questionnaire distributed among employees. Due to internal reasons, it was not possible to apply all the above elements at all three participating organisations. A comprehensive implementation could only be achieved at APG, while ÖBB merely allowed the application of some of the above elements. WIGEV was analysed using exclusively qualitative interviews and an assessment of documents. Following our analysis, each organisation received the results in a confidential report.

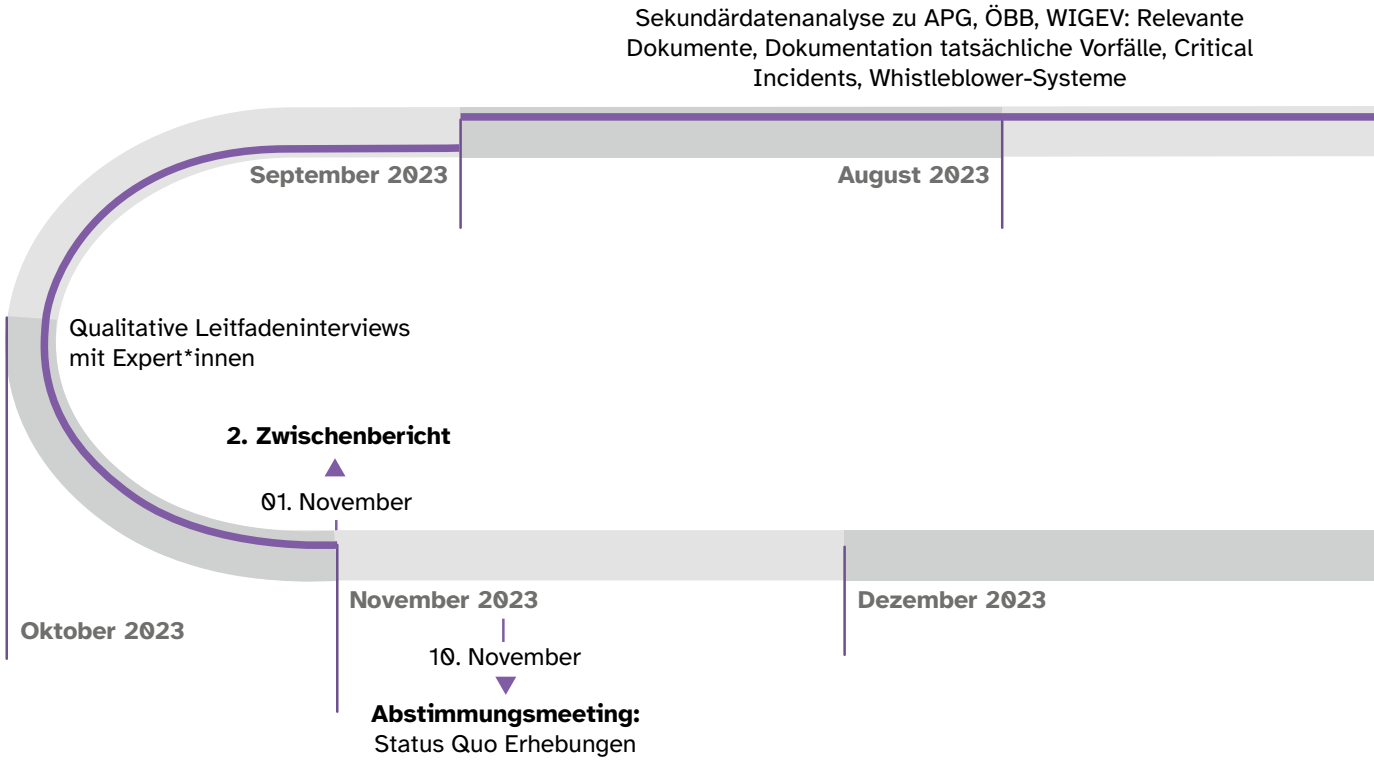
In a workshop, the findings were discussed with security officers from different critical infrastructure sectors. This resulted in the joint development of recommendations for a general improvement of security culture.

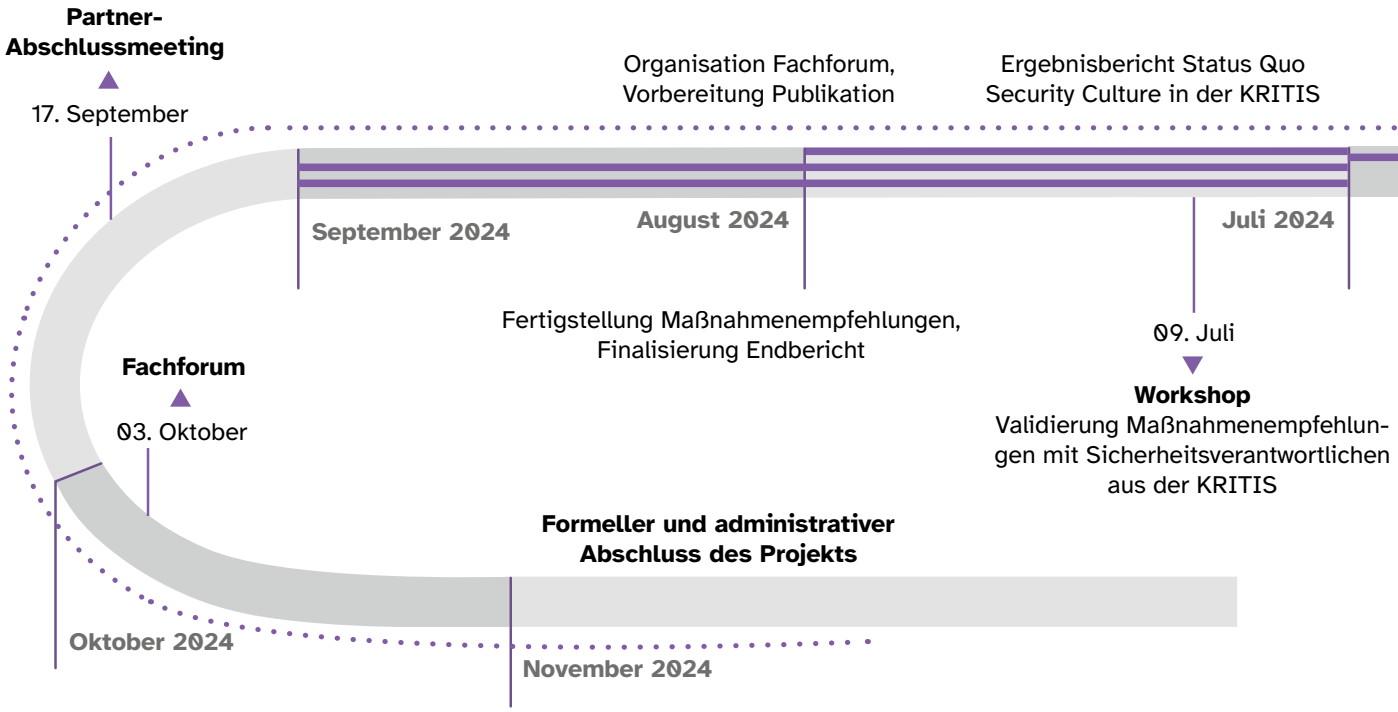
The final project report contains a summary of the findings from the quantitative and qualitative analyses of the three partner organisations and general recommendations for measures to improve the security culture of the critical infrastructure.

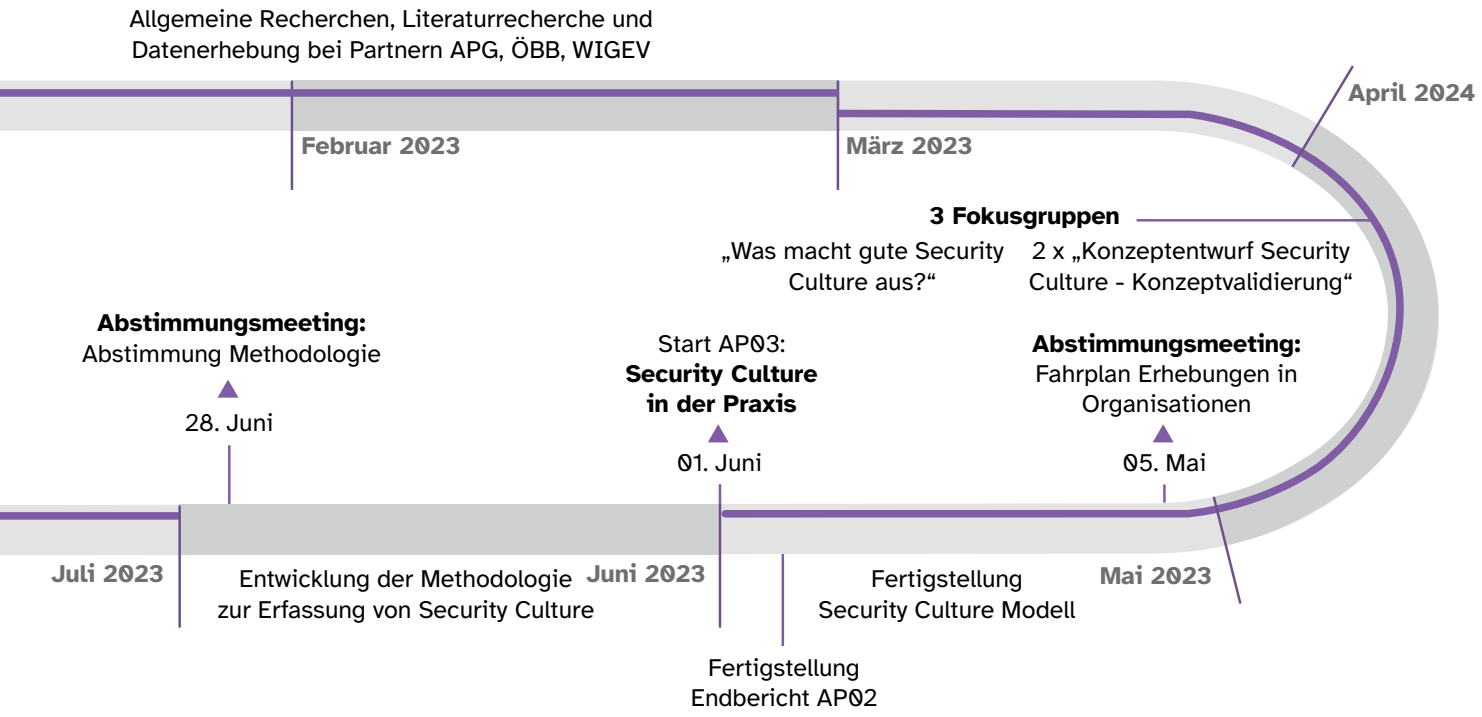
PROJEKTVERLAUF

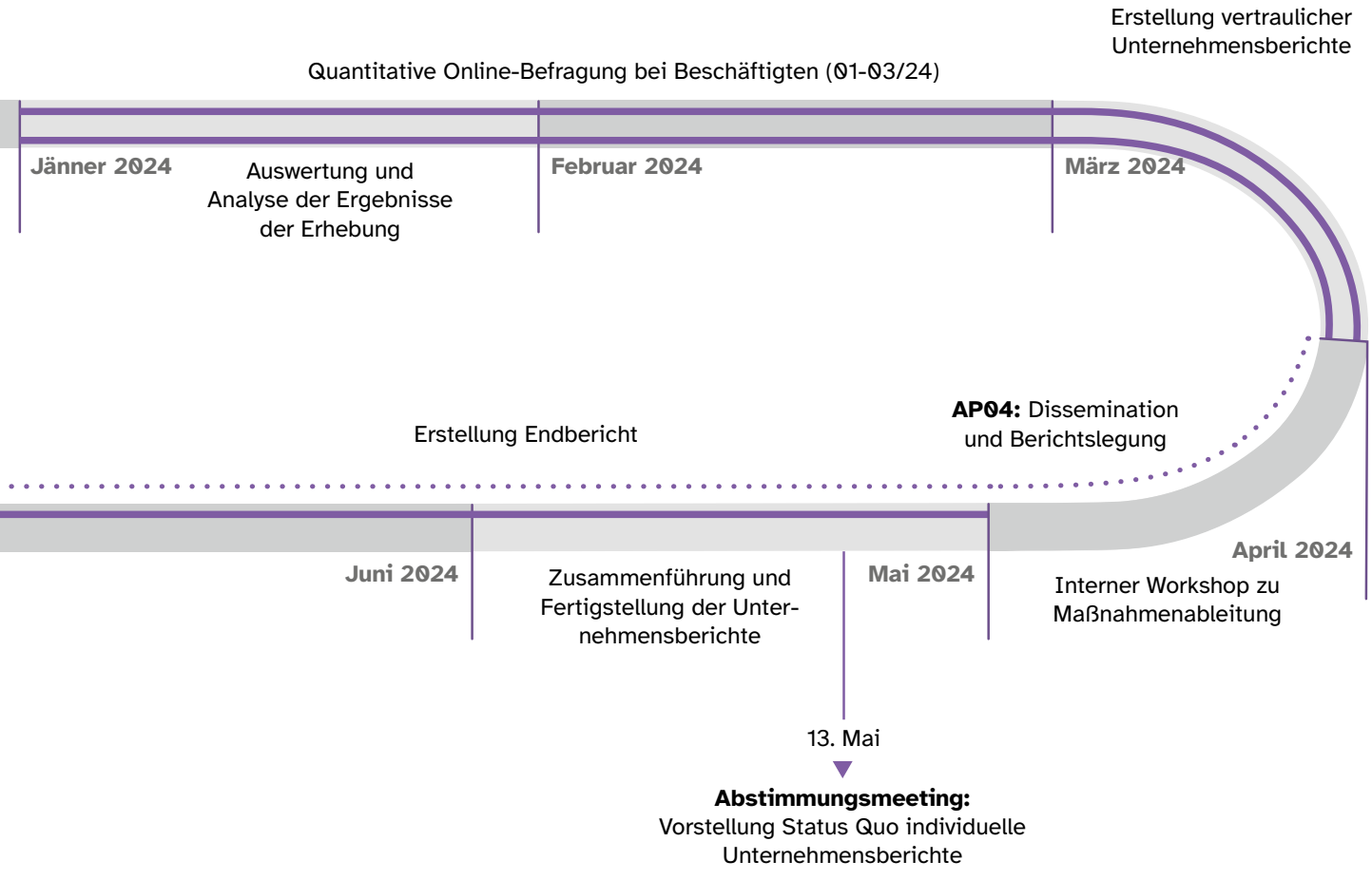
November 2022 - November 2024








Allgemeine Recherchen, Literaturrecherche und Datenerhebung bei Partnern APG, ÖBB, WIGEV
Februar 2023
März 2023
April 2024
3 Fokusgruppen
„Was macht gute Security Culture aus?“
2 x „Konzeptentwurf Security Culture - Konzeptvalidierung“
Abstimmungsmeeting: Abstimmung Methodologie
28. Juni
Start AP03: Security Culture in der Praxis
01. Juni
Abstimmungsmeeting: Fahrplan Erhebungen in Organisationen
05. Mai
Juli 2023
Entwicklung der Methodologie zur Erfassung von Security Culture
Juni 2023
Fertigstellung Security Culture Modell
Mai 2023
Fertigstellung Endbericht AP02


Erstellung vertraulicher Unternehmensberichte
Quantitative Online-Befragung bei Beschäftigten (01-03/24)
Jänner 2024
Auswertung und Analyse der Ergebnisse der Erhebung
Februar 2024
März 2024
AP04: Dissemination und Berichtslegung
Erstellung Endbericht
April 2024
Juni 2024
Zusammenführung und Fertigstellung der Unternehmensberichte
Mai 2024
Interner Workshop zu Maßnahmenableitung
13. Mai
Abstimmungsmeeting: Vorstellung Status Quo individuelle Unternehmensberichte

STATEMENTS


JKU

Univ.-Prof. Dr.
Helmut Hirtenlehner
Johannes Kepler
Universität Linz

Als Kriminologe sehe ich täglich, dass Sicherheit ein wichtiges Gut darstellt. Das gilt auch und besonders für den Bereich der Kritischen Infrastruktur. Hier würden Funktionsausfälle für große Teile der Bevölkerung erhebliche Probleme schaffen. Die entsprechenden Institutionen werden daher gut beraten sein, sich gegen Sicherheitslücken zu wappnen, indem sie das Sicherheitsbewusstsein ihrer Mitarbeiterinnen und Mitarbeiter stärken und deren Identifikation mit den geltenden Sicherheitsregeln festigen.

Die vorliegende Forschung will diesen Prozess durch evidenzbasierte Analysen der betrieblichen Sicherheitskulturen unterstützen.


Lischka

Gerald Lischka, BA MA
Abteilungsleiter für Schutz
und Sicherheit im Bundes-
ministerium für Inneres

Kritische Infrastrukturen sind ein wesentlicher Bestandteil zur Aufrechterhaltung wichtiger gesellschaftlicher Funktionen. Mit der nationalen Umsetzung der Richtlinie zur Resilienz Kritischer Einrichtungen (RKE) soll mittels verpflichtender Maßnahmen, sowohl für den Staat als auch für die Unternehmen, das Resilienz-Niveau erhöht werden. Zu den verpflichtenden Maßnahmen auf Unternehmensseite zählt unter anderem die Meldung von erheblichen Sicherheitsvorfällen an die staatlich zuständige Behörde.

Um Sicherheitsvorfälle auch im Zusammenhang mit intentionalen Gefahren erkennen und richtig einordnen zu können, bedarf es einer entsprechenden Sicherheitskultur im Unternehmen. Die Erkenntnisse von SiKu KRITIS fördern die Weiterentwicklung der Sicherheitskultur in Unternehmen der Kritischen Infrastruktur und sind ein wichtiger Beitrag zur Erhöhung der Resilienz im Zusammenhang mit aktuellen und künftigen Krisen.


Ricardo Herrgott

DI Mag. (FH)
Gerhard Christiner
APG, Technischer Vorstand

Das Thema „Sicherheitskultur in der Kritischen Infrastruktur“ könnte kaum relevanter sein, insbesondere in einer Zeit, in der die Herausforderungen in unserer zunehmend vernetzten und komplexen Welt immer größer werden. Die sichere Stromversorgung bildet das Rückgrat unserer modernen Gesellschaft. Vor allem die versorgungssichere Energieversorgung ist essenziell für die Elektrifizierung von Gesellschaft, Industrie und Wirtschaft.

Im Rahmen des Forschungsprojektes der FH Campus Wien wurde intensiv untersucht, wie die Sicherheitskultur in unserem Unternehmen verankert ist, welche Faktoren sie beeinflussen und welche Strategien zu ihrer Verbesserung beitragen können. Die gewonnenen Erkenntnisse bieten wertvolle Einblicke und praxisnahe Empfehlungen, die uns helfen werden, unsere Sicherheitskultur noch sicherer zu machen.

Die Zusammenarbeit mit der FH Campus Wien hat uns gezeigt, wie fruchtbar der Austausch zwischen Wissenschaft und Praxis sein kann. Dafür möchte ich allen Beteiligten, insbesondere den Projektverantwortlichen der FH Campus Wien, meinen herzlichen Dank aussprechen.


ÖBB

DI Mark Topal-Gökceli
Leiter ÖBB Systemtechnik und Konzernproduktion


ÖBB

Roman Hahslinger, BA MA
CSO – Chief Security Officer ÖBB

Die Sicherheitskultur in der Kritischen Infrastruktur ist von wesentlicher Bedeutung für den Schutz der Gesellschaft. Eine starke Sicherheitskultur umfasst das Bewusstsein und die Bereitschaft aller Mitarbeiterinnen und Mitarbeiter, Sicherheitsrisiken zu erkennen und diese täglich proaktiv zu minimieren.

Es beginnt schon bei der Schulung und Sensibilisierung aller Beteiligten und erstreckt sich über die Implementierung entsprechender Leitlinien und Regelwerke bis zur kontinuierlichen Überprüfung der Maßnahmen.

Führungskräfte spielen dabei eine zentrale Rolle, indem sie ein Umfeld schaffen, in dem Sicherheitsfragen offen angesprochen und kontinuierlich verbessert werden können.

Ein wichtiger Unternehmensgrundsatz der ÖBB lautet „Sicherheit Leben“ und zielt vor allem auf die Vorbildwirkung aller Mitarbeiterinnen und Mitarbeiter ab. Zudem ist die Zusammenarbeit mit externen Partnerinnen und Partnern sowie Behörden unerlässlich, um Bedrohungen frühzeitig zu erkennen und abzuwehren. Eine widerstandsfähige Sicherheitskultur ist daher nicht nur eine Frage der Technik, sondern auch des menschlichen Faktors und der institutionellen Zusammenarbeit. Sie bildet das Fundament, auf dem der sichere Betrieb Kritischer Infrastrukturen beruht und trägt wesentlich zur Stabilität und Widerstandsfähigkeit der Gesellschaft bei.


Christof Peter

Christof Peter, BSc MA MSc
Wiener Gesundheitsverbund, Vorstandsressort Qualität, Prävention und Sicherheit

Die Sicherheitskultur ist im WIGEV bereits stark ausgeprägt, dennoch konnte das KIRAS-Projekt noch Verbesserungspotentiale identifizieren, welche die Unternehmung in die kontinuierliche Weiterentwicklung mitaufgenommen hat. Eine Herausforderung stellt die Verknüpfung von Sicherheitsmaßnahmen mit den Hauptaufgaben aller Mitarbeiterinnen und Mitarbeiter dar. Dafür setzt der WIGEV , wie auch die Studie empfiehlt, auf qualifiziertes, praxisorientiertes Personal, damit gezielte und klare Abläufe zu keiner Sicherheitsfrustration aller Personen in unseren Einrichtungen führt.

Eine weitere Herausforderung ist die Durchführung von wiederkehrenden und verpflichtenden Sensibilisierungs- und Schulungsmaßnahmen auf allen Hierarchieebenen. Diese sind für eine lebendige Sicherheitskultur unabdingbar. Der Ansatz, Sicherheitskultur messbar und damit vergleichbar zu machen, gewinnt mit der Umsetzung der Richtlinien NIS2 und RKE eine noch höhere Bedeutung. Danke für die Möglichkeit zur Mitwirkung an diesem Projekt.


APG

SECURITY CULTURE: RECHTLICHE RAHMENBEDINGUNGEN, THEORETISCHE KONZEPTUALISIERUNG UND EMPIRISCHE ERGEBNISSE

NORMATIVE RAHMENBEDINGUNGEN

Rechtliche Rahmenbedingungen für den Bereich der Kritischen Infrastruktur gibt es sowohl auf nationaler als auch auf unionsrechtlicher Ebene. Die nationalen Gesetze müssen dabei die Vorgaben der EU erfüllen. Daher sind neue Bestimmungen auf Grundlage einer EU-RL zu erlassen und bereits bestehende gesetzliche Regelungen sind entsprechend anzupassen. Keiner nationalen Umsetzung bedürfen lediglich EU-VO, die in den Mitgliedstaaten unmittelbar gelten.

Auf unionsrechtlicher Ebene wurden für die Sicherheit Kritischer Infrastrukturen folgende RL erlassen:

- EPCIP-RL (RL 2008/114/EG)
- RKE-Richtlinie (RL 2022/2557)
- NIS-Richtlinie (RL 2016/1148)
- NIS-2-Richtlinie (2022/2555)
- Straftatbestände RL (2013/40/EU)

Bislang (Stand 15. Juli 2024) hat Österreich nur die EPCIP-RL, die NIS-RL und die RL für die Erweiterung der Straftatbestände umgesetzt. Auf Grundlage der NIS-RL hat der österreichische Gesetzgeber das NISG erlassen und zusätzlich wurde österreichweit das APCIP geschaffen, welches ein Programm zum Schutz Kritischer Infrastrukturen darstellt und auf freiwilliger Basis aufbaut.

Aufgrund der NIS-2-RL und der RKE-RL wird der österreichische Gesetzgeber noch bis Oktober 2024 die nationale Umsetzung in die Rechtsordnung realisieren.

KONZEPTUALISIERUNG SICHERHEITSKULTUR

Die Begriffe Safety und Security werden in verschiedenen Kontexten und Disziplinen unterschiedlich definiert. Safety konzentriert sich hauptsächlich auf die Vermeidung von Unfällen, während Security den Schutz vor Angriffen betont.

- Safety wird oft mit „Betriebssicherheit“ übersetzt und bezieht sich auf technische und natürliche Gefahren.
- Security wird hingegen als „Angriffssicherheit“ verstanden und meint also etwa den Schutz vor Vorfällen von Cyberkriminalität, Betrug oder Diebstahl.

Im Rahmen einer ausführlichen Literaturrecherche konnten bestehende relevante Modelle zu Security und Safety in Organisationen identifiziert werden. Anhand von drei Fokusgruppen diskutierten Sicherheitsverantwortliche Fragen wie: Was alles gehört zu einer (guten) Sicherheitskultur einer Organisation? Welche Elemente machen Sicherheitskultur aus und wodurch werden sie beeinflusst? Aufbauend auf den Ergebnissen der Fokusgruppen wurde ein Modell für Security Culture entwickelt, welches die Einflussfaktoren auf Security Culture transparent macht und als Grundlage für die folgenden empirischen Erhebungen im AP03 diente.

Die untenstehende Abbildung veranschaulicht die Abgrenzung und Überschneidung der beiden Begriffe Safety und Security. Im Projekt SiKu KRITIS lag der Fokus auf Security.

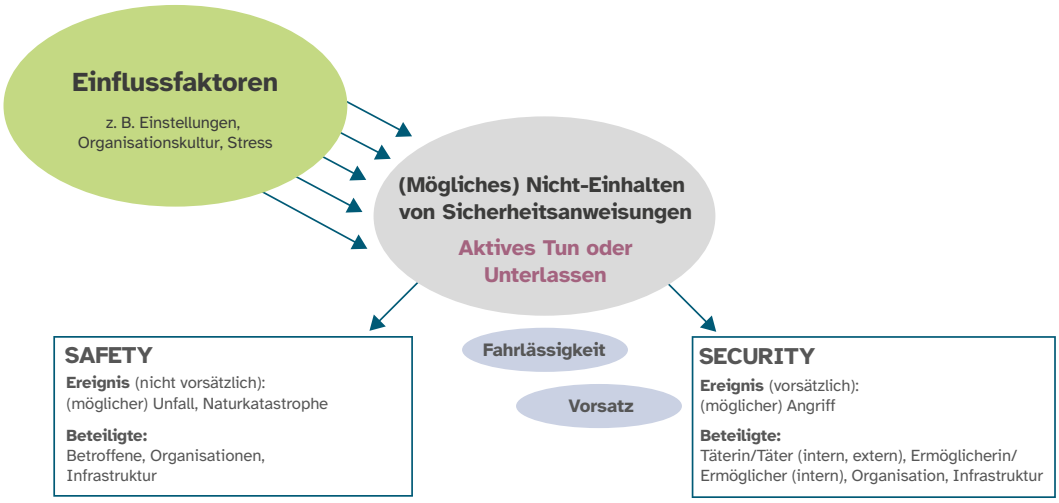


Abbildung: Begriffsklärung Safety und Security

SECURITY bezieht sich auf den Schutz vor vorsätzlichen Bedrohungen. Empfehlungen und Vorschriften zum Schutz vor Angriffen sowie das Verhalten der Beschäftigten in Bezug auf diese Regeln prägen die Sicherheitskultur. Das Nicht-Einhalten von Sicherheitsvorschriften im Bereich Security durch Mitarbeiterinnen und Mitarbeiter begünstigt Sicherheitsvorfälle. Diese können aufgrund von Unterlassen, Fahrlässigkeit oder Vorsatz eintreten, sowohl von Personen innerhalb als auch außerhalb einer Organisation. An Sicherheitsvorfällen beteiligte Personen können Täterinnen und Täter sowie gegebenenfalls Ermöglicherinnen und Ermöglicher innerhalb der Organisation sein, die durch die Nicht-Einhaltung von Sicherheitsregeln das Eintreten solcher Vorfälle erleichtern. Auch eine Organisation selbst kann durch formelle und informelle Rahmenbedingungen sowie ihre physische Infrastruktur Vorfälle begünstigen oder verhindern.

Die folgende Abbildung zeigt jenes „Security Culture"-Modell, das im Rahmen des vorliegenden Projekts auf Grundlage vorhandener theoretischer Modelle und empirischer Erkenntnisse entwickelt wurde.

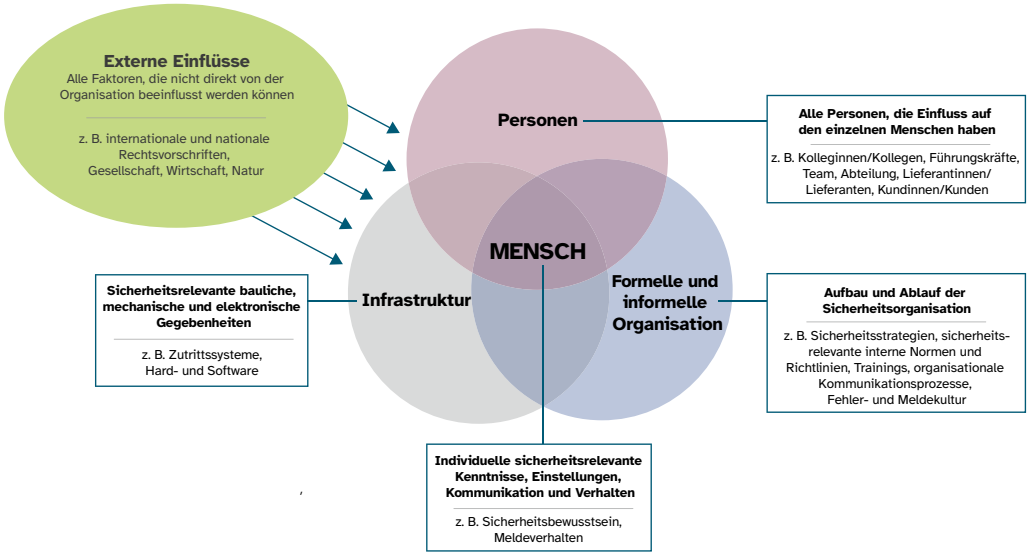


Abbildung: Konzeptualisierung Security Culture

Die **SECURITY CULTURE** einer Organisation wird von vier inneren kulturprägenden Faktoren beeinflusst:

- Formelle und informelle Organisation
- Infrastruktur der Organisation
- Andere Organisationsmitglieder
- Mensch

Darüber hinaus spielen externe Faktoren, wie z. B. internationale und nationale Rechtsvorschriften, gesellschaftliche und politische Rahmenbedingungen sowie natürliche Gegebenheiten eine Rolle.

ÖBB

METHODISCHE VORGEHENSWEISE: QUANTITATIVE UND QUALITATIVE ERHEBUNGEN

Die qualitativen Erhebungen erstreckten sich über einen Zeitraum von Sommer 2023 bis Anfang 2024: Bei den Unternehmen fanden Fokusgruppen mit Mitarbeitenden und mit Sicherheitsverantwortlichen sowie qualitative leitfadengestützte Interviews mit Führungskräften statt.

Die den qualitativen Interviews zugrundeliegenden Leitfäden wurden in Work Group Meetings innerhalb des Projektteams sowie in Abstimmungsmeetings mit den Projektpartnerinnen und Projektpartnern besprochen sowie gegebenenfalls adaptiert.

Es wurden u.a. folgende Fragen in den Interviews behandelt:

- Wie wichtig ist aus Ihrer Sicht das Thema Sicherheit für Ihren Bereich und warum?
- Mit welchen Bedrohungen sehen Sie Ihren Bereich im Sinne von Angriffssicherheit konfrontiert?
- Was macht aus Ihrer Sicht Security Culture aus?
- Welche Rolle spielt hier Kommunikation allgemein im Unternehmen?

Im Rahmen der Fokusgruppen wurde u.a. über die folgenden Themen diskutiert:

- Wenn Sie an Mitarbeiterinnen und Mitarbeiter denken: Was sind aus Ihrer Sicht die wichtigsten Einflussfaktoren bei Sicherheitsvorfällen? (Kenntnisse, Einstellungen und Verhalten von Mitarbeiterinnen und Mitarbeitern)
- Was könnte Sicherheitsverhalten fördern?
- Wie schätzen Sie die Klarheit und das Ausmaß von offiziellen Vorgaben und Richtlinien im Bereich Security in Ihrem Unternehmen ein?
- Wie beurteilen Sie die Sicherheitskultur in Ihrem Unternehmen?

Darüber hinaus erfolgte eine quantitative Erhebung bei den Beschäftigten von APG und ÖBB anhand eines Online-Fragebogens. Die Items des Fragebogens wurden basierend auf theoretischen Überlegungen und Konzeptionalisierungen aus dem Arbeitspaket 02 formuliert.

WIGEV/Kromus

Anhand der Situational Action Theory (SAT) von Wikström und der Neutralisierungsthese von Sykes und Matza wurden die Fragen und Items des Fragebogens in Zusammenarbeit mit dem Projektpartner Johannes Kepler Universität Linz gestaltet und gemeinsam mit den beteiligten Unternehmen im Rahmen von Pretests u.a. auf ihre Praxistauglichkeit geprüft.

Die Befragung wurde internetbasiert als Online-Survey mit Hilfe des Tools TIVIAN von Jänner bis März 2024 durchgeführt.

Bezogen auf die Anzahl an Personen, an die der Link zum Fragebogen ausgesendet wurde, haben bei den ÖBB in einem Unternehmensstandort rund 17 % den Fragebogen beendet. Hier ist anzumerken, dass der Fragebogenlink nicht an die Grundgesamtheit (alle Beschäftigten), sondern per Schneeballverfahren durch das Unternehmen ausgesendet wurde.

Bei der APG konnte eine Beendigungsquote von etwa 29 % realisiert werden, wobei hier der Link durch das Unternehmen an die Grundgesamtheit verschickt wurde.

SITUATIONAL ACTION THEORY (SAT)
von Per-Olof H. Wikström (2004)

Die Situational Action Theory (SAT) des schwedischen Kriminologen Wikström (Universität Cambridge) ist eine allgemeine Theorie abweichenden oder normwidrigen Handelns. Die Theorie will erklären, warum Menschen Verhaltensregeln verschiedenster Art übertreten. Starke Moralvorstellungen, hohe Selbstkontrolle, ein der Norm verbundenes moralisches Umfeld und intakte Sanktionierungsrisiken wirken dem Verletzen von Verhaltensregeln entgegen. Die SAT konnte inzwischen eine Fülle von bestätigenden Evidenzen anhäufen.

NEUTRALISIERUNGSTECHNIKENTHESE
von Gresham M. Sykes und David Matza (1957)

Immer wieder kann beobachtet werden, dass Menschen Normen verletzen, die sie eigentlich verinnerlicht haben, also akzeptieren und gutheißen. Die situative Aufhebung grundsätzlich internalisierter Verhaltensstandards steht im Mittelpunkt der sogenannten Neutralisationstechnikenthese. Neutralisationstechniken – also Techniken zur Rechtfertigung abweichenden Verhaltens im Einzelfall – dienen der Auflösung des Paradoxons aus Anerkennung und gleichzeitiger Übertretung einer Norm.
Als gelernte „Ausreden“ oder „Entschuldigungen“ ermöglichen sie ein vorübergehendes Ausschalten moralischer Hemmungen und versetzen Menschen so in die Lage, Regeln zu verletzen, die sie prinzipiell akzeptieren.

ERGEBNISSE DER QUALITATIVEN ERHEBUNGEN

Die Ergebnisse der qualitativen Erhebungen lassen auf ein hohes Sicherheitsverständnis in den beteiligten Organisationen schließen. Die Sicherheitskultur wird von den befragten Unternehmen als hoch ausgeprägt angesehen. Dennoch scheint Verbesserungspotenzial gegeben zu sein. Das Vorhandensein von Richtlinien und offiziellen Vorgaben wird positiv hervorgehoben. Laut den Teilnehmerinnen und Teilnehmern bei den Interviews und Fokusgruppen ist eine Vielzahl an Sicherheitsrichtlinien etabliert. Dabei wird vor allem die „Lebbarkeit" von Richtlinien in der Praxis hervorgehoben, welche ein wichtiges Kriterium seitens der Beschäftigten darstellt.

Dementsprechend sollten Richtlinien nicht allzu komplex gestaltet werden. Außerdem wird in den Erhebungen betont, dass Richtlinien teilweise klarer formuliert und deren Einhaltung von der Führungsebene strenger kontrolliert werden sollten. Darüber hinaus wird konstatiert, dass es wünschenswert wäre, die Vermittlung bzw. Bekanntgabe von Richtlinien transparenter zu gestalten. Weiters zeigt sich ein wesentlicher Einfluss des „Tone from the Top" auf das Verhalten bzw. Handeln der einzelnen Mitarbeiterinnen und Mitarbeiter.

Hinsichtlich des Objektschutzes sind Defizite vorhanden. Dies lässt auf informelle Prozesse und Strukturen in den befragten Unternehmen schließen. Vor allem, wenn offizielle Richtlinien nicht lebbar zu sein scheinen, werde nach „Workarounds" gesucht. Zudem können Überlastung und Stress der Belegschaft die Wahrscheinlichkeit erhöhen, dass die Einhaltung von Sicherheitsvorschriften im Bereich Objektschutz der Betriebs- und Arbeitssicherheit sowie der Sicherheit von Patientinnen und Patienten untergeordnet wird.

Die Ergebnisse der qualitativen Erhebungen zeigen außerdem, dass den Mitarbeiterinnen und Mitarbeitern die Vorgaben zum Schutz vor physischen Angriffen einerseits oftmals inhaltlich nicht ausreichend klar und andererseits aufgrund mangelnder Kommunikation nicht immer bekannt sind. Zur Schärfung des Sicherheitsbewusstseins wünschen sich die Beschäftigten praxisnahe Beispiele.

Die Fehlerkultur wird überwiegend positiv erlebt. Es gehe vor allem darum, Fehler offen anzusprechen und eine Person nicht zu diffamieren, sollte ein Fehler passiert sein. In den Erhebungen wurde die Wichtigkeit einer offenen Fehlerkultur für das Melden von Vorfällen bzw. Fehlern betont. Es hänge stark von der Führungskraft ab, wie auf Fehler reagiert wird. Das Ansprechen von Fehlverhalten durch Kolleginnen und Kollegen wird von Beschäftigten oftmals als unangenehm empfunden. Daher werden jene Mitarbeiterinnen und Mitarbeiter, die sich nicht an interne Sicherheitsanweisungen halten, zumeist nicht darauf hingewiesen. Somit herrscht hinsichtlich dieses Aspekts ein eher heterogenes Bild in den Unternehmen.

Hinsichtlich Bedrohungen sehen sich die Unternehmen weniger mit Bedrohungen von innen, dafür umso mehr mit externen Gefahren, wie Spionage oder Hackerangriffen, konfrontiert. Bei externen Faktoren, wie Krieg und Terrorismus, sieht man sich auf staatliche Hilfe angewiesen.

APG

ERGEBNISSE DER QUANTITATIVEN ERHEBUNGEN

In der Befragung der Mitarbeiterinnen und Mitarbeiter mittels Online-Fragebogen zeigt sich, dass dem Faktor Sicherheit hohe Wichtigkeit zugeschrieben wird. Annähernd alle Antwortenden geben jeweils an, dass Sicherheit im Arbeitsalltag eine wesentliche Rolle spielt. Des Weiteren legen die Ergebnisse nahe, dass ein hohes Maß an Sicherheitsbewusstsein in den jeweiligen Unternehmen etabliert ist. Das Gros der Studienteilnehmerinnen und -teilnehmer akzeptiert bzw. befürwortet die vorhandenen Sicherheitsregeln.

Verbesserungspotenzial kann bei Maßnahmen zum physischen Objektschutz konstatiert werden. Fast alle an der Umfrage teilnehmenden Personen sind sich bewusst, welche Konsequenzen vonseiten des Unternehmens drohen würden, wenn sie sich nicht an die unternehmensinternen Sicherheitsvorschriften und -regelungen halten.

Mitarbeiterinnen und Mitarbeiter berichten Vorgesetzten während der täglichen Arbeit nicht oft über sicherheitsrelevante Themen. Es zeigt sich aber, dass Sicherheitsverstöße sehr wohl häufig bekannt gegeben werden. Rund zwei Drittel melden Sicherheitsvorfälle immer, wenn diese bemerkt werden. Hier sind Unterschiede zwischen verschiedenen Organisationseinheiten erkennbar. Hinsichtlich der Einschätzung der Nützlichkeit der etablierten Sicherheitsmaßnahmen geben die Studienteilnehmerinnen und -teilnehmer an, dass diese überwiegend als sinnvoll erachtet werden. Bei der subjektiven Wahrnehmung, wie oft Mitarbeiterinnen und Mitarbeiter über bestimmte Sicherheitsthemen informiert werden, rangieren Cyber- und Informationssicherheit sowie Arbeitnehmerschutz an den vordersten Stellen. Vor allem zu den Themen Cyber-, Informationssicherheit und Objektschutz werden mehr Informationen gewünscht.

Als geeignetes Kommunikationsmedium dafür werden u.a. jährliche Unterweisungen, Intranet-Beiträge und anlassbezogene Sicherheitshinweise genannt. Hinsichtlich der zukünftigen Herausforderungen, mit denen sich die Belegschaft der Unternehmen konfrontiert sieht, lässt sich feststellen, dass Cybersicherheit die größte subjektiv wahrgenommene Gefahr darstellt.

ZUSAMMENFASSUNG DER ERGEBNISSE

Wie die Analyse der im Rahmen des Projektes übermittelten internen Dokumente (Richtlinien und Maßnahmen) zeigt, scheinen in zwei der insgesamt drei teilnehmenden Unternehmen die unternehmensinternen Richtlinien und Maßnahmen für die Umsetzung der externen Vorgaben zu genügen.

Aktuell (Stand 15. Juli 2024) bleibt offen, wie die „neuen“ Richtlinien, RKE-RL und NIS-2, in Österreich umgesetzt werden und ob dafür weitere unternehmensinterne Richtlinien und Maßnahmen nötig bzw. bereits bestehende Regelungen anzupassen sind.

In den Ergebnissen der qualitativen und quantitativen Erhebungen in den Partnerorganisationen des Forschungsprojektes wird ersichtlich, dass die Sicherheitskultur in den ausgewählten Unternehmen bereits gut ausgeprägt ist.

Die während der qualitativen und quantitativen Erhebungen in den jeweiligen Unternehmen gewonnenen Erkenntnisse wurden in vertraulichen Unternehmensberichten festgehalten. Darüber hinaus wurden basierend auf den Ergebnissen Empfehlungen bzw. Maßnahmenvorschläge zur Verbesserung der Sicherheitskultur ausgearbeitet und beschrieben.


ÖBB
3 - 12
InfoPoint
Sonnwendgasse
WC

EMPFEHLUNGEN

Basierend auf den Ergebnissen der vorliegenden Untersuchung eignen sich die in der folgenden Abbildung dargestellten Empfehlungen zur Verbesserung der Security Culture in der KRITIS.

Abbildung: Empfehlungen zur Verbesserung der Security Culture

1. Security Awareness und „Tone from the Top“ – wesentliche Faktoren der Unternehmenssicherheit
Laut aktuellem Forschungsstand handeln Mitarbeiterinnen und Mitarbeiter mit einem höheren Wissensstand und einer positiveren Einstellung gegenüber Security (höheres Sicherheitsbewusstsein) auch sicherheitskonformer. Wissen kann als zentrale Komponente für Security Awareness betrachtet werden.

Folgende Empfehlungen zur Steigerung der Security Awareness können für Unternehmen abgeleitet werden:

- Wissensvermittlung durch Sicherheitsexpertinnen und -experten zu den Themen Spionage, Sabotage, Diebstähle und Übergriffe anhand „typischer“ Beispiele. Ob die Wissensvermittlung in Präsenz oder online erfolgt, ist vor allem zielgruppenorientiert zu entscheiden (abhängig von Berufsgruppe, Gruppengröße etc.). Auch Externe sollen in die Wissensvermittlung einbezogen werden.
- Einsatz von Gamification, um realistische Situationen erlebbar zu machen und dadurch Betroffenheit zu vermitteln und die Security Awareness zu fördern.
- Etablierung kurzer Inputs zu Sicherheitsthemen durch Führungskräfte („Tone from the Top“).

2. Sicherheitsrichtlinien und Handlungsanweisungen geben Orientierung
Ein weiteres wichtiges Element zum Schutz vor Angriffen im Rahmen der formellen und informellen Organisation ist die Implementierung und Gestaltung von Sicherheitsrichtlinien und Handlungsanweisungen, die den realen Bedrohungen von Unternehmen entsprechen. Adäquate Sicherheitsrichtlinien und Handlungsanweisungen geben Orientierung und unterstützen sicherheitskonformes Handeln. Fehlen konkrete Vorgaben, so können Mitarbeiterinnen und Mitarbeiter präventive Schutzmaßnahmen nicht korrekt anwenden und in Angriffssituationen nicht wie vom Unternehmen gewünscht reagieren.
Bei der Verinnerlichung von Sicherheitsrichtlinien bzw. -maßnahmen durch Mitarbeiterinnen und Mitarbeiter spielen die Akzeptanz und die Ansicht, dass die Richtlinien notwendig sind, eine wesentliche Rolle.
Folgende Empfehlungen zur verbesserten Gestaltung von Richtlinien und Handlungsanweisungen können aus dem Projekt abgeleitet werden:

- Wiederholte Durchsicht und gegebenenfalls Anpassung der Sicherheitsrichtlinien und Handlungsanweisungen an relevante Bedrohungen (Reduzierung oder Ergänzung von Vorgaben)

- Sprachliche Barrieren bei Richtlinien und Handlungsanweisungen vermeiden. Die Ergänzung mit Piktogrammen kann dabei positiv sein, wobei auch auf mögliche kulturell unterschiedliche Bedeutungszuschreibungen zu achten ist.
- Bei der Gestaltung von Sicherheitsrichtlinien und Handlungsanweisungen ist auf folgende Kriterien zu achten:
    - Titel
    - Klare Zielsetzung
    - Begründungen für eine Richtlinie
    - Definition der Zielgruppe
    - Übersichtlichkeit der Inhalte

3. Umsetzung von Identifikations- und Zugangskontrollmaßnahmen

Ein wichtiges Element zum Schutz vor Angriffen sind Zugangsbeschränkungen und die Identifikation von Organisationsmitgliedern im Unternehmen. Zur Abwehr von Spionage, Sabotage und Diebstählen ist es entscheidend zu wissen, welche Personen sich wo in der Organisation aufhalten. Zugangsbeschränkungen und Identifikation von Mitarbeiterinnen und Mitarbeitern werden neben einer physischen Zugangskontrolle oftmals durch technische Lösungen sowie Identitätsnachweise, wie z.B. Videoüberwachung, Tragen von Lanyards und den Einbau von Vereinzelungsanlagen, unterstützt. Für die Akzeptanz dieser Tools spielt die benutzerfreundliche Gestaltung (neben der Security Awareness) eine große Rolle – dazu bietet sich die Anwendung von „Nudging“ an.

Bezüglich der Umsetzung von Identifikations- und Zugangskontrollmaßnahmen können folgende Empfehlungen gegeben werden:

- Benutzerfreundliches Gestalten von Identifikationsmaßnahmen zur Verbesserung der Nutzung, wie z. B. durch Verwendung bequemer Materialien für Lanyards und Einsatz von Zusatzfunktionen (z.B. Mitarbeitendenkarte mit Schließfunktion, um den persönlichen Nutzen für Mitarbeiterinnen und Mitarbeiter zu erhöhen).
- Technische Konzipierung von Objektschutzmaßnahmen gemäß dem Stand der Technik, um nur sicherheitskonformes Handeln zu ermöglichen. Mit Hilfe von Druckpunkten am Boden kann beispielsweise sichergestellt werden, dass nur eine Person die Vereinzelungsanlage passieren kann.

NUDGING
von Richard Thaler & Cass Sunstein (2008)

Die Idee des Nudging wurde von Thaler und Sunstein, zwei US-amerikanischen Verhaltensökonomen, in ihrem Buch „Nudge: Wie man kluge Entscheidungen anstößt“, beschrieben. Durch sogenannte Nudges werden Individuen sanft zu erwünschten Verhaltensweisen geleitet. 2017 erhielten sie den Wirtschaftsnobelpreis für diese Idee.


ÖBB

4. Positive Fehlerkultur als Grundlage für das Melden von Vorfällen

Wie gehen Mitarbeiterinnen und Mitarbeiter selbst und wie gehen Organisationen mit Fehlern um? Werden Fehler offen angesprochen, um daraus zu lernen, oder werden sie verheimlicht, um mögliche soziale und organisationale Sanktionen abzuwenden? Werden Fehler als Lernchance und Ansatz für Verbesserungen begriffen, so sind auch Mitarbeiterinnen und Mitarbeiter motivierter und es entstehen Möglichkeiten für Fortschritte. Gespräche darüber und Befragungen der Belegschaft können sich ebenfalls positiv auf die Fehlerkultur auswirken.

Folgende Empfehlungen können eine positive Fehlerkultur fördern:

- Offener Umgang mit Fehlern und Beinahe-Vorfällen („Weak Signals“) durch entsprechende strategische Vorgaben für Führungskräfte, zur Unterstützung des „Tone from the Top“ und der Mitarbeiterinnen und Mitarbeiter.
- Auseinandersetzung mit der Nicht-Einhaltung von Sicherheitsanweisungen und den diesbezüglichen Rechtfertigungen auf Ebene der Sicherheitsverantwortlichen und Führungskräfte.
- Fortbildungen und Schulungen zum Thema Fehlerkultur vor allem für Führungskräfte.
- Etablierung einer „lernenden Organisation“ durch Einbettung von Fehlermeldungen und Beinahe-Vorfällen in einen kontinuierlichen Verbesserungsprozess, durch den aufgetretene Fehler und Beinahe-Vorfälle analysiert werden und Lernprozesse entstehen.
- Möglichst einfache Gestaltung des Erstmeldeprozesses von Fehlern.
- Keine Sanktionen bei Meldung von Fehlern. Hingegen sollten bewusst nicht gemeldete Fehler sanktioniert werden.

5. Sicherheitskonformes Handeln gestaltet Security Culture

Security Culture wird durch das Handeln von Mitarbeiterinnen und Mitarbeitern in Übereinstimmung mit sicherheitsrelevanten Handlungsanweisungen und Richtlinien gelebt. Dieses basiert idealerweise auf einem Sicherheitsbewusstsein, das sich auf realistische Bedrohungen bezieht, sowie dem Wissen und der Fähigkeit, sicherheitskonformes Handeln umsetzen zu können.

Folgende Maßnahmen eignen sich, um sicherheitskonformes Handeln und damit Security Culture zu fördern:

- Vermittlung von Wissen durch Expertinnen und Experten zu den typischen Vorgehensweisen im Rahmen von Angriffen für alle Beschäftigten.
- Definition von Personen, die als Unterstützung für Mitarbeiterinnen und Mitarbeiter bei Antreffen einer unternehmensfremden Person ohne Identifikationsnachweis fungieren und dafür mittels Verhaltenstraining geschult sind. Grundsätzlich sollte jede/r Mitarbeiterin und Mitarbeiter unternehmensfremde Personen ohne Identifikationsnachweis ansprechen.

REFLEXION UND AUSBLICK

Die Erforschung der Organisationskultur eines Unternehmens setzt Offenheit für tiefe Einblicke in formale und informale Strukturen und Abläufe voraus. In dieser Studie wurden sowohl qualitative als auch quantitative Methoden angewendet, um Führungskräfte und Beschäftigte zu befragen, sowie vertrauliche sicherheitsrelevante Dokumente analysiert. Dies diente dazu, ein umfassendes Bild der Security Culture in ausgewählten Organisationen der KRITIS zu erhalten.

Die Unterstützung durch Führungskräfte in Unternehmen sowie das Schaffen einer vertrauensvollen Basis von Seiten der Forscherinnen und Forscher ist bei solchen Vorhaben grundlegend. Ohne diese Grundvoraussetzungen können keine wissenschaftlich verwertbaren Ergebnisse erzielt werden. Daher müssen vor Beginn solcher Untersuchungen entsprechende Rahmenbedingungen von sämtlichen Beteiligten geklärt und sichergestellt werden, um eine effiziente und effektive Durchführung des Forschungsvorhabens zu gewährleisten.

Dies ist besonders für die Durchführung von repräsentativen Befragungen der Mitarbeiterinnen und Mitarbeiter wichtig, die dazu dienen, Hypothesen aus den qualitativen Daten zu überprüfen und wichtige Einblicke in die Security Culture zu erhalten.

Im vorliegenden Projekt haben sich die qualitativen und quantitativen Erhebungen als besonders herausfordernd erwiesen. Aus diesem Grund müssen die Ergebnisse mit Vorbehalt betrachtet werden.

Dieses Projekt bietet Einblicke in die Security Culture ausgewählter Organisationen und ist ein erster Schritt zur Beschreibung der Security Culture in der KRITIS in Österreich. Es stellt eine theoretische Grundlage und methodische Herangehensweise bereit, die als Modell für weitere Studien dienen kann. Zur Gewinnung umfassenderer Erkenntnisse wäre es nun sinnvoll, zusätzliche Erhebungen in Unternehmen aus weiteren Sektoren der KRITIS durchzuführen, um vergleichende Analysen zu ermöglichen.

ÖBB

DAS PROJEKTTEAM

PROJEKTLEITUNG


FH Campus Wien Schedl

FH-PROF.IN MAG.A CLAUDIA KÖRMER
ist seit Sommer 2014 an der FH Campus Wien im Fachbereich Risiko- und Sicherheitsmanagement in Forschung und Lehre tätig. Sie hat eine Reihe von nationalen und internationalen sozialwissenschaftlichen Projekten erfolgreich geleitet und umgesetzt, darunter „Wirtschafts- und Industriespionage in österreichischen Unternehmen 2010 und 2015“, „Konzernsicherheit in der D-A-CH Region“, die KIRAS-Projekte AQUS, AQUS II sowie ESBH (ab November 2022). Davor war die studierte Soziologin 17 Jahre lang in den Bereichen Verkehrssicherheit, Heim-, Freizeit- und Sportunfälle sowie Kriminalität im Kuratorium für Verkehrssicherheit tätig. claudia.koermer@fh-campuswien.ac.at

WEITERS IM PROJEKTTEAM


privat/zVg

MIRJAM JOHANNA HABISREUTINGER, MA
ist seit November 2022 im Forschungsteam des Fachbereichs Risiko- und Sicherheitsmanagement an der FH Campus Wien tätig. Hier organisiert und forscht sie insbesondere im Rahmen von KIRAS-Projekten. Die Absolventin des Masterstudiums der Kultur- und Sozialanthropologie war davor als Verwaltungspraktikantin im Bundesministerium für Landesverteidigung tätig.


Kristina Hauer

KRISTINA HAUER, BA
verstärkt seit Sommer 2023 das Team des Fachbereichs als wissenschaftliche Mitarbeiterin. Ihr Interesse an quantitativen Methoden und Mixed-Methods-Studien kann die studierte Soziologin in diversen Forschungsprojekten einbringen. Dazu zählen neben den laufenden KIRAS-Projekten auch ein Umfrageprojekt zu Wirtschafts- und Industriespionage 2024 in Österreich.

JOHANNES KEPLER
UNIVERSITÄT LINZ

JKU

UNIV.-PROF. DR. HELMUT HIRTENLEHNER
ist Leiter des Zentrums für Kriminologie der Johannes Kepler Universität Linz. Seine Habilitation für Kriminalsoziologie und Kriminologie erfolgte 2008. Seine Forschungsschwerpunkte liegen im Bereich Kriminalitätsfurcht, Sanktionsforschung, kriminologische Theorieprüfung und quantitative Kriminologie. Im KIRAS-Projekt SiKu KRITIS brachte er soziologische und kriminologische Expertise ein. helmut.hirtenlehner@jku.at

Michaela Kerschbaummaier

MAG.A DR.IN LISA SCHMOLLMÜLLER
ist seit 2016 als Universitätsassistentin am Institut für Strafrechtswissenschaften der JKU tätig. Seit 2022 ist sie primär dem neu gegründeten Institut für Procedural Justice zugeordnet. Ihre Forschungsschwerpunkte umfassen das Strafverfahrensrecht, den allgemeinen Teil des Strafrechts sowie die empirische Rechtstatsachenforschung. Bei SiKu KRITIS brachte sie ihre juristische Expertise und ihre Kompetenzen in der Datenanalyse ein.

Fotostudio Eder

MAG.A LAURA HAUSER
ist seit 2022 als Universitätsassistentin am Institut für Strafrechtswissenschaften der JKU tätig. Zuvor absolvierte sie das Studium der Rechtswissenschaften an der JKU. Sie sammelte bereits während ihres Studiums Erfahrungen als studentische Mitarbeiterin am Institut für Strafrechtswissenschaften und am Institut für Staatsrecht und politische Wissenschaften. Ihre Forschungsarbeit konzentriert sich primär auf Fragestellungen im Bereich des Strafverfahrensrechts und des besonderen Teils des Strafrechts. Bei SiKu KRITIS hat sie ihre juristische Expertise aktiv eingebracht.

DANKSAGUNG
Herzlichen Dank an alle Expertinnen und Experten in Institutionen, Branchennetzwerken, Bundesministerien und weiteren Behörden, Unternehmen und Organisationen, die zu den Ergebnissen dieses Projekts durch wertvolle Informationen, Einschätzungen und weitere Kontakte beigetragen haben.

SIKU KRITIS (2022-2024)

PROJEKTKONSORTIUM

FH Campus Wien
Johannes Kepler Universität Linz
Wirtschaftskammer Österreich
Austrian Power Grid AG
Österreichische Bundesbahnen
Wiener Gesundheitsverbund

Via Letter of Intent eingebunden:
A1 Telekom Austria AG
Österreichischer Rundfunk

Bundesministerium für Inneres
Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
Bundesministerium für Klimaschutz, Umwelt, Energie, Umwelt, Innovation und Technologie

Bundesministerium
Inneres

Bundesministerium
Soziales, Gesundheit, Pflege
und Konsumentenschutz

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie