SiKu KRITIS

Konzeptualisierung und Erhebung der Sicherheitskultur in der Kritischen Infrastruktur

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, KIRAS F&E-Dienstleistungen 2021	**Status**	abgeschlossen
Projektstart	02.11.2022	**Projektende**	01.11.2024
Zeitraum	2022 - 2024	**Projektlaufzeit**	25 Monate
Keywords	Sicherheitskultur, Kritische Infrastruktur		

Projektbeschreibung

Die Kritische Infrastruktur (KRITIS) stellt einen besonders sensiblen Bereich des österreichischen Staates dar. Als ein zentraler Faktor für den Schutz der KRITIS gilt die Sicherheitskultur in Organisation. Sicherheitskultur in Organisationen wurde bisher hauptsächlich in Zusammenhang mit Unfällen erforscht. Aber, wie die aktuellen Krisen zeigen, vor allem intentionale Gefahren, wie Wirtschafts- und Industriespionage, Korruption, Veruntreuung, Cyberangriffe, Diebstähle und Übergriffe auf Mitarbeiter:innen sind zunehmende Bedrohungen für Organisationen der KRITIS. Einige wenige Ansätze zur Messung des Begriffs Security Culture wurden in den letzten zehn Jahren entwickelt. Bisher gibt es aber keinen Ansatz der eine breite wissenschaftliche Konzeptualisierung von Security Culture bietet, ausreichend als Basis für empirische Forschung geeignet wäre und relevante kriminologische Perspektiven, wie die Situational Action Theory von Wikström (2015) sowie die Neutralisationstechnikenthese von Sykes und Matza (1957) zur Erklärung von normwidrigem Verhalten von Mitarbeiter:innen inkludiert. Security Culture kann dadurch bis dato nicht wissenschaftlich erfasst und gestaltet werden.
Der theoretische Fokus des geplanten Vorhabens liegt daher auf einer umfassenden empirisch relevanten Konzeptualisierung von Security Culture. Diese theoretische Konzeptualisierung wird durch Sicherheitsverantwortliche im Hinblick auf ihre praktische Relevanz validiert (AP2). Im empirischen Teil wird die Sicherheitskultur in Organisationen der KRITIS mit dem Fokus auf intentionale Gefahren erstmalig erhoben und analysiert. Davon umfasst ist die Erforschung der Compliance der Mitarbeiter:innen bezogen auf innerbetriebliche Sicherheitsnormen und die Erklärung von etwaigen Verstößen. Jeweils ein Unternehmen aus den zur Zeit durch die Krisen besonders betroffenen KRITIS-Sektoren Gesundheit, Energie und Mobilität soll mittels einem im Projekt entwickelten Mixed-Method-Ansatz aus qualitativer Analyse von sicherheitsrelevanter Infrastruktur und Dokumenten, qualitativen Befragungen von relevanten Schlüsselpersonen sowie Führungskräften und standardisiertem Fragebogen für Mitarbeiter:innen untersucht werden (AP3). Die Erkenntnisse, die aus den aggregierten Ergebnissen gewonnen werden, dienen dazu Empfehlungen für die gesamte KRITIS abzuleiten und fließen in eine Publikation ein, die bei einer Fachkonferenz vorgestellt wird. Die Projektergebnisse werden in diesem Rahmen mit Sicherheitsverantwortlichen und –expert:innen diskutiert (AP4).

Abstract

Critical infrastructure is a particularly sensitive area of the Austrian state. A central factor for the protection of critical

infrastructure is the safety culture in organisations. Safety culture in organisations has so far mainly been used in connection with accidents. But, as the current crises show, especially intentional threats such as economic and industrial espionage, corruption, embezzlement, cyber attacks, thefts and assaults on employees are increasing threats to critical infrastructure organisations. A few approaches to measuring the concept of security culture have been developed over the last decade. So far, however, there is no approach that offers a broad scientific conceptualisation of security culture, is sufficiently suitable as a basis for empirical research and includes relevant criminological perspectives such as Wikström's Situational Action Theory (2015) and Sykes and Matza's Neutralisation Technique Thesis (1957) to explain normative behaviour by employees. As a result, security culture cannot yet be scientifically captured and shaped.
The theoretical focus of the planned project is therefore on a comprehensive, empirically relevant conceptualisation of "security culture". This theoretical conceptualisation will be validated by security managers with regard to its practical relevance (WP2). In the empirical part, the security culture in critical infrastructure organisations is surveyed and analysed for the first time with a focus on intentional threats. This includes research into the compliance of employees with regard to internal security standards and the explanation of any violations. One company from each of the crisis-affected critical infrastructure sectors - health, energy and mobility - will be investigated using a mixed-method approach developed in the project consisting of qualitative analysis of security-relevant infrastructure and documents, qualitative interviews with relevant key persons and managers, and a standardised questionnaire for employees (WP3). The findings obtained from the aggregated results will be used to derive recommendations for the entire critical infrastructure and will be included in a publication that will be presented at a conference. The project results will be discussed with security managers and experts (WP4).

Projektkoordinator

- Hochschule für Angewandte Wissenschaften Campus Wien (HCW)

Projektpartner

- Austrian Power Grid AG
- Universität Linz Zentrum für Kriminologie
- Wiener Gesundheitsverbund
- Wirtschaftskammer Österreich
- Österreichische Bundesbahnen-Holding Aktiengesellschaft