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).

Endberichtkurzfassung

Im Rahmen des Projektes "Sicherheitskultur in der Kritischen Infrastruktur - SiKu KRITIS" konnten folgende zentrale Projektergebnisse erzielt werden:

Ein erstes wichtiges Projektergebnis ist ein Überblick über Richtlinien auf unionsrechtlicher Ebene , die für die Sicherheit Kritischer Infrastrukturen erlassen wurden:

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)

Ein weiteres bedeutendes Projektergebnis ist eine Grafik der Konzeptualisierung der Security Culture in Organisationen. Diese Grafik (siehe Endbericht AP04 und Publikation) zeigt, dass die Security Culture einer Organisation von vier inneren kulturprägenden Faktoren beeinflusst wird:

Formelle und informelle Organisation

Infrastruktur der Organisation
Andere Organisationsmitglieder
Individuum

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

Die Analyse, der im Rahmen des Projektes von den Partnerorganisationen übermittelten securityrelevanten Richtlinien und Maßnahmen , weist darauf hin, dass in zwei der insgesamt drei befragten Unternehmen die unternehmensinternen Richtlinien und Maßnahmen für die Umsetzung der externen Vorgaben genügen. In einem der drei Unternehmen ist es jedoch nicht möglich, umfassende Aussagen darüber zu treffen, ob die zurzeit existierenden Richtlinien und Maßnahmen zur Umsetzung der externen Vorgaben ausreichend sind. Außerdem 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.

Die zentralen Ergebnisse der qualitativen und quantitativen Erhebungen in den Partnerorganisationen des Forschungsprojektes, die auf der Konzeptualisierung von Security Culture beruhen, zeigen, dass die Sicherheitskultur in den ausgewählten Unternehmen bereits gut ausgeprägt ist. Im Zusammenhang mit Cyber-, Informationssicherheit und Arbeitnehmer:innenschutz fühlen sich die Mitarbeiter:innen von den Unternehmen zumeist gut informiert. Die Bereiche Betriebssicherheit und Arbeitssicherheit sind im Bewusstsein der Führungskräfte und Mitarbeiter:innen besonders gut verankert, dies zeigt sich ebenfalls in bereits gut etablierten Sicherheitsmaßnahmen. Vor allem bei der Akzeptanz von Objektschutzmaßnahmen hat die Security Culture noch Nachholbedarf. Obwohl Mitarbeitende grundsätzlich mit den vorhandenen physischen Sicherheitsmaßnahmen einverstanden sind, sind sie manchmal nicht bereit, diese einzuhalten bzw. umzusetzen. Diese werden häufig als wenig praktisch, unangenehm oder sogar störend empfunden. Wie von den Mitarbeitenden empfohlen, könnte sich das Unternehmen in Bezug auf Security an den anderen Sicherheitsbereichen orientieren und im Bereich Objektschutz Schwerpunkte in Bezug auf Bewusstseinsbildung, Information und benutzerfreundliche Gestaltung setzen. Wenn die Security Culture in den Unternehmen hoch sein und somit der Schutz vor Angriffen bestmöglich gewährleistet werden soll, muss sie ganzheitlich gedacht werden. Eine Zusammenarbeit zwischen den verschiedenen Bereichen, wie Informationssicherheit, IT-Sicherheit und Objektschutz, ist wesentlich, um Lücken in der Sicherheit identifizieren und schließen zu können.

Folgende hauptsächliche Empfehlungen zur Verbesserung der Security Culture in der KRITIS wurden auf Basis der zentralen Ergebnisse des AP03 identifiziert (siehe Überblicksgrafik Endbericht AP04 und Publikation):

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.

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

Folgende grundlegende Überlegungen ergaben sich im Rahmen einer abschließenden Projektreflexion und dienen als Ausblick für weitere Forschung:

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.

Projektkoordinator

- Hochschule für Angewandte Wissenschaften Campus Wien (HCW)

Projektpartner

- Bundeshauptstadt Wien
- Wirtschaftskammer Österreich
- Österreichische Bundesbahnen-Holding Aktiengesellschaft
- Universität Linz
- Austrian Power Grid AG