

CLEAR-CHAIN

CLEAR-CHAIN

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, KIRAS CS F&E-Dienstleistungen (CS FED_2025)	Status	laufend
Projektstart	01.10.2026	Projektende	30.09.2027
Zeitraum	2026 - 2027	Projektlaufzeit	12 Monate
Barwert der Projektförderung	€ 199.838		
Keywords	IKT-Lieferkettensicherheit; Cybersicherheit; NIS-2-Richtlinie; Risikoreferenzmodell; Digitale Souveränität		

Projektbeschreibung

Die Sicherheit von Lieferketten für Informations- und Kommunikationstechnologien (IKT) ist eine zentrale Voraussetzung für die Funktionsfähigkeit digitaler Dienste und damit für Staat, Wirtschaft und Gesellschaft. Insbesondere öffentliche und private Einrichtungen, die wesentliche und wichtige Dienste im Sinne der NIS-2-Richtlinie erbringen, sind auf vertrauenswürdige, transparente und resiliente IKT-Lieferketten angewiesen, um ihre Leistungen dauerhaft gegen Cyberangriffe, Manipulationen und Ausfälle abzusichern.

Vor diesem Hintergrund zielt das Projekt CLEAR-CHAIN darauf ab, einen fundierten Beitrag zur Erstellung eines nationalen Konzepts für die Cybersicherheit in der Lieferkette von IKT-Produkten und IKT-Diensten gemäß Art. 7 Abs. 2 lit. a der NIS-2-Richtlinie als Bestandteil der nationalen Cybersicherheitsstrategie zu leisten. Die Studie adressiert den Bedarf, sicherheitsrelevante Risiken in zunehmend komplexen, häufig international verzweigten IKT-Lieferketten systematisch zu erfassen, zu bewerten und auf den österreichischen Kontext zu übertragen, sodass konkrete Umsetzungsanforderungen und anschlussfähige Leitlinien abgeleitet werden können.

Ziel der Studie ist die strukturierte Identifikation, Bewertung und Priorisierung von Bedrohungsszenarien, typischen Angriffsvektoren, Schwachstellen, kritischen Abhängigkeiten und Schutzbedarf entlang der IKT-Lieferkette. Dabei wird untersucht, wie technische, organisatorische, regulatorische und geopolitische Faktoren zur Entstehung von Risiken beitragen und wie sich diese auf die Resilienz und Funktionsfähigkeit von Einrichtungen auswirken. Besonderes Augenmerk liegt auf Abhängigkeiten von bestimmten Anbietern, Technologien oder Herkunftsländern sowie auf Risiken durch kompromittierte oder manipulierte Produkte und Dienstleistungen.

Aufbauend auf einer systematischen Analyse bestehender regulatorischer, normativer und technischer Maßnahmen sowie international bewährter Frameworks und Modelle wird deren Wirksamkeit und praktische Umsetzbarkeit bewertet und es werden bestehende Umsetzungsprobleme identifiziert. Ergänzend werden Transparenz, Herkunftsnachweis und

Nachvollziehbarkeit in der Lieferkette aus technischer, organisatorischer und regulatorischer Perspektive analysiert. Empirische Erkenntnisse aus Expert:inneninterviews, Umfragen und strukturierten Austauschformaten mit relevanten Stakeholdern fließen in die Bewertung ein und ermöglichen eine praxisnahe Einordnung.

Die Ergebnisse des Projekts umfassen einen national angepassten Bedrohungs- und Risikokatalog für IKT-Lieferketten, Modelle zur systematischen Risikoidentifikation und -bewertung sowie rechtlich fundierte, umsetzungsorientierte Handlungsempfehlungen. Darüber hinaus werden Ansätze zur Verbesserung der Zusammenarbeit und des Informationsaustauschs zwischen Einrichtungen, Lieferanten und Dienstleistern sowie zur Stärkung der Cybersicherheitskultur entlang der Lieferkette (zB durch Schulungen, Audits, Zertifizierungen und vertragliche Anforderungen) abgeleitet. CLEAR-CHAIN schafft damit eine belastbare fachliche Grundlage für politische Entscheidungsprozesse und unterstützt die Stärkung der nationalen Cybersicherheits- und Resilienzstrategie. Die Projektergebnisse verstehen sich als Elemente für eine Policy-Grundlage und stellen ausdrücklich kein Werkzeug oder Produkt dar, das die Einhaltung gesetzlicher Vorgaben (insbesondere NISG 2026) nahelegt oder bescheinigt.

Abstract

The security of supply chains for information and communication technology (ICT) is a fundamental prerequisite for the reliable provision of digital services and, consequently, for the functioning of government, the economy and society. In particular, public and private entities providing essential and important services within the meaning of the NIS2 Directive depend on trustworthy, transparent and resilient ICT supply chains in order to effectively protect their services against cyberattacks, manipulation and disruptions.

Against this background, the project CLEAR-CHAIN contributes to the development of a national concept for cybersecurity in the supply chain of ICT products and ICT services in accordance with Article 7(2)(a) of the NIS2 Directive, as part of the national cybersecurity strategy. The study addresses the need to systematically identify and assess security-relevant risks in increasingly complex and often internationally distributed ICT supply chains and to adapt them to the Austrian context, enabling the derivation of concrete implementation requirements and nationally applicable guidelines. The objective of the study is the structured identification, assessment and prioritization of threat scenarios, typical attack vectors, vulnerabilities, critical dependencies and protection needs along the ICT supply chain. In this context, the study examines how technical, organizational, regulatory and geopolitical factors contribute to the emergence of risks and how these risks affect the resilience and operational continuity of entities. Particular attention is paid to dependencies on specific vendors, technologies or countries of origin, as well as to risks arising from compromised or manipulated products and services.

Building on a systematic analysis of existing regulatory, normative and technical measures, as well as internationally established frameworks and models, their effectiveness and practical applicability are assessed, and existing implementation challenges are identified. In addition, transparency, provenance and traceability within the supply chain are analyzed from technical, organizational and regulatory perspectives. Empirical insights from expert interviews, surveys and structured stakeholder exchange formats are incorporated to ensure a practice-oriented assessment.

The project results include a nationally adapted ICT supply chain threat and risk catalogue, models for the systematic identification and assessment of risks, and legally sound, implementation-oriented recommendations for action. Furthermore, approaches to improving cooperation and information exchange between entities, suppliers and service

providers, as well as to strengthening the cybersecurity culture along the supply chain (e.g. through training, audits, certifications and contractual requirements), are derived. CLEAR-CHAIN thus provides a robust analytical basis for policy decision-making and supports the strengthening of the national cybersecurity and resilience strategy. The project results are intended as elements for a policy basis and explicitly do not constitute a tool or product that implies or certifies compliance with legal requirements (in particular the NISG 2026).

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Bundesministerium für Inneres
- Bundesministerium für Innovation, Mobilität und Infrastruktur (BMIMI)
- Bundesministerium für Landesverteidigung
- Bundesministerium für Wirtschaft, Energie und Tourismus
- Kompetenzzentrum Sicheres Österreich (KSÖ)
- PwC Wirtschaftsprüfungs- und Steuerberatungsgesellschaft mbH
- Research Institute AG & Co KG
- SBA Research gemeinnützige GmbH
- Österreichische Agentur für Gesundheit und Ernährungssicherheit GmbH