SOPHIE

reSilienz vOn supPly cHaIns gegenüber kaskadEneffekten aus dem digitalen Raum

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIras Kooperative CS F&E Projekte (KFE CS_2022)	**Status**	laufend
Projektstart	01.11.2023	**Projektende**	30.06.2026
Zeitraum	2023 - 2026	**Projektlaufzeit**	32 Monate
Keywords	Cyber Security, Supply Chain, Modellierung, Kaskadeneffekte, Schulung, Weiterbildung		

Projektbeschreibung

Die Resilienz von IKT-Infrastrukturen ist fundamental für das Funktionieren von Supply Chains. Je verlässlicher diese Infrastrukturen sind, desto höher ist auch die Planbarkeit für Produktion und Lieferketten, und daraus resultierend für die Abnehmer:innen und Kund:innen. Die Absicherung solcher Systeme gegen Bedrohungen aus dem Cyberraum ist zentral für das Funktionieren einer „Smart Economy“, die auf dem Prinzip „Just in Time“ aufbaut und möglichst ohne Zwischenlagerung auskommen Transportwege optimieren muss. Im Fall eines Cyber-Angriffes ist es essentiell, auf bewährte Strukturen und Prozesse, ausreichende Früherkennung und entsprechende Entscheidungsmodelle zurückgreifen zu können, um Beeinträchtigungen von IKT-Systemen möglichst zu vermeiden bzw. zu reduzieren.
Das Projekt SOPHIE zielt daher darauf ab, Bewusstsein für Themen der Cyber Security in der Supply Chain, des Incident Response insbesondere für technisches und nicht-technisches Schlüsselpersonal in der Supply Chain zu steigern, sowie relevante Prozesse durch geeignete Tools und Referenzprozesse im Sinne der Resilienz zu unterstützen und zu verbessern.
Das Projekt verfolgt drei wesentliche Ziele:
(1) die Auswirkungen von Cyberangriffen besser zu verstehen,
(2) die Anzahl und Kritikalität erfolgreicher Cyberangriffe zu vermindern und
(3) die Aufklärungsrate bei Cyberangriffen zu steigern und den Aufwand für Angriffe präventiv signifikant zu erhöhen.
Diese Ziele soll SOPHIE durch korrespondierende Maßnahmen erreichen, insbesondere:
(1) die Analyse von Prozessen, Kaskadeneffekte und geeignete Verfahren, um Modelle für Übungen und Simulationen von Cyber-Vorfällen zu erstellen, (2) im Rahmen von Übungen und Simulationen rasch und wirkungsvoll auf IT-Sicherheitsvorfälle zu reagieren, um letztlich
(3) die Auswirkungen von Sicherheitsvorfällen zu minimieren, Schwachstellen zu beheben, sowie die Robustheit und Resilienz der Systeme zu erhöhen.

SOPHIE wird hierfür die Prozesse zur Analyse, Modellbildung und Simulation in Schulungsprogramme und Cyber-Security Übungen zur Bewusstseinsbildung einsetzen. Dies soll helfen, die Verhaltensweisen der Anwender:innen im Ernstfall zu reflektieren, operative und Entscheidungsprozesse zu analysieren, und geeignete Maßnahmen des Krisenmanagement zu definieren und zu validieren, sowie die Koordination zwischen Akteur:innen und deren Verantwortlichkeiten zu koordinieren.

Ergänzend dienen die Simulationsmodelle hier auch der Identifizierung kritischer Prozesse, sowie der Erkennung etwaiger Ressourcen- und Kapazitätsengpässe, woraus relevante Möglichkeiten zur taktischen Optimierung von Prozessen abgeleitet werden. Dies soll zu einem proaktiven und reaktiven Umgang mit Cyber-Attacken durch Unternehmen entlang einer Supply Chain beitragen.

Abstract

The resilience of ICT infrastructures is fundamental to the functioning of supply chains. The reliability of these infrastructures increases the reliability of planning for production and supply chains, as well as for customers and demanders. The protection of such systems against threats from cyber space is central to the functioning of a "smart economy", which is based on the principle of "just in time", characterised by very short intermediate storage times and the optimization of supply routes. In the event of a cyber-attack, it is essential to be able to rely on established strategies and processes, effective early detection and adequate decision-making models in order to avoid or reduce disruptions to ICT systems as far as possible.
The SOPHIE project aims at increasing awareness of cyber security issues in the supply chain and incident response, especially for technical and non-technical core staff, as well as supporting and improving relevant processes by implementing suitable tools and reference processes for building resilience. The project has three main objectives:
(1) improving the understanding of impacts of cyber-attacks,
(2) reducing the number and criticality of successful cyber-attacks and
(3) raising the reconnaissance rate of cyber-attacks and significantly increasing the cost of attacks in a preventive manner.
SOPHIE will achieve these goals through corresponding measures, in particular:
(1) the analysis of processes, cascade effects and suitable procedures to create models for exercises and simulations of cyber incidents, to
(2) react promptly and effectively to IT security incidents within the framework of exercises and simulations, and ultimately to
(3) minimise the impact of security incidents, remedy vulnerabilities, and enhance the robustness and resilience of systems.

SOPHIE will use the analysis, modelling and simulation processes in training programmes and cyber security awareness exercises for this purpose. This shall help to reflect the behaviour of users in the case of an emergency, to analyse operational and decision-making processes and to define and validate appropriate response measures as well as to coordinate actors and their responsibilities. In addition, the simulation models also facilitate the identification of critical processes, as well as the recognition of possible resource and capacity bottlenecks, from which relevant opportunities for the tactical optimisation of processes are derived. This contributes to the proactive and reactive handling of cyber-attacks by companies along a supply chain.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- h2 projekt.beratung KG
- Bundeskanzleramt
- Digital Factory Vorarlberg GmbH

- Institut für empirische Sozialforschung (IFES) Gesellschaft mbH
- Bundesministerium für Wirtschaft, Energie und Tourismus
- FH OÖ Forschungs & Entwicklungs GmbH
- Bundesministerium für Landesverteidigung
- Gebrüder Weiss Gesellschaft m.b.H.
- Universität für Bodenkultur Wien
- Bundesministerium für Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft
- CER Cargo Traction GmbH
- Universität Linz
- Bundesministerium für Inneres