Cyber.LWS

Cybersicherheit und Resilienz landwirtschaftlicher Prozesse und Systeme zur Gewährleistung der Versorgungssicherheit

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, KIRAS-Kybernet-Pass CS F&E Dienstleistungen (CS FED_2024)	**Status**	laufend
Projektstart	01.10.2025	**Projektende**	30.09.2027
Zeitraum	2025 - 2027	**Projektlaufzeit**	24 Monate
Keywords	Cybersicherheit, Landwirtschaft, Versorgungssicherheit, Resilienz, Risikoanalyse		

Projektbeschreibung

Das Projekt Cyber.LWS (Wiedereinreichung aus dem Jahr 2024) zielt darauf ab, durch eine systematische Bedrohungsanalyse und zielgerichtete Sicherheitsstrategien die Cybersicherheit und Resilienz landwirtschaftlicher Betriebe in Österreich zu erhöhen. Damit wird ein wesentlicher Beitrag zur Wettbewerbsfähigkeit und Versorgungssicherheit geleistet.

Cyber.LWS führt erstmals eine sektorspezifische Cybersicherheitsbetrachtung für die österreichische Landwirtschaft durch, indem es bereits existierende Sicherheitskonzepte und Methoden aus anderen Bereichen (z. B. dem Automotive-Sektor) systematisch auf landwirtschaftliche Use Cases und Betriebsstrukturen überträgt.

Statt einer generischen Betrachtung fokussiert sich Cyber.LWS auf verschiedene Betriebsarten und -größen sowie unterschiedliche Digitalisierungslevels. Ziel ist es, neben der Bedrohungsanalyse, eine landwirtschaftsspezifische Bedrohungsdatenbank im Tool ThreatGet zu erstellen, um weitere Systeme, auch nach Ende des Projekts, automatisiert analysieren zu können.

Dazu sollen im Projekt die folgenden Fragestellungen beantwortet werden:
- Welche Cyberbedrohungen sind für die Landwirtschaft relevant und wie können Angreifer konkret vorgehen?
- Wo liegen die Verwundbarkeiten und welche Folgen/Auswirkungen können auf Betriebe bzw. auf die Versorgungssicherheit entstehen?
- Welche übergeordneten Gegenmaßnahmen (Schulungen, regulatorische Vorgaben (Abschätzung Relevanz CRA, UN R155, NIS2)) können zur Risikominimierung gesetzt werden und wer trägt hier die Verantwortung?
- Wie lassen sich die Ergebnisse in nationale Programme durch politische Entscheidungsträger:innen einbinden?
- Welche übergeordneten Strategien für Landwirt:innen, Hersteller und Staat, unter Einbeziehung relevanter Regelwerke können für künftige Sicherheitsstandards im Agrarsektor entwickelt werden?

Besonders für die folgenden Stakeholder ist ein nachhaltiger Nutzen durch das Projekt zu erwarten:
- Landwirt:innen: Skalierbare Präventionsmaßnahmen durch niederschwellige Lösungen wie Schulungen,

Sensibilisierungsprogramme und Checkliste, sowie Fokus auf grundlegende IT Sicherheitsmaßnahmen
- Dienstleister/Hersteller: Empfehlungen zu Hardware- und Software-Sicherheitsanforderungen, die sich an bestehenden Strategien (z. B. Cyber Resilience Act, Nationale IKT-Sicherheitsstrategie) orientieren sowie Ansätze für Zertifizierungs- und Testverfahren, um Manipulationen und Angriffsszenarien präventiv zu unterbinden.
- Regierungsorganisationen: Möglichkeiten zur Integration der Ergebnisse in nationale Programme (z.B. Fördersystem) zur langfristigen und flächendeckenden Umsetzung sowie Nutzung der ThreatGet-Analysen und Projektresultate als Basis für politische Maßnahmen, gesetzliche Richtlinien und Förderinhalte.

Das Projekt stärkt somit die Cyberresilienz und Versorgungssicherheit in Österreich.

Nach einem Feedbacktermin mit der FFG wurden die folgenden Anpassungen in der Wiedereinreichung vorgenommen:
- Der Innovationsgehalt wurde klarer herausgearbeitet und die Verwertungspotenziale konkretisiert.
- Die Planung und Methodenauswahl wurden präzisiert, die Arbeitspakete strukturiert und die Ressourcen für die Schwachstellenanalyse erweitert.
- Relevante Ergebnisse aus Vorprojekten wurden konkreter dargestellt.
- Die Ressourcenverteilung wurde nach kritischer Evaluation angepasst.
- Das Nutzenversprechen wurde deutlicher formuliert.
- Die Genderausgewogenheit im Team wurde verbessert

Abstract

The project Cyber.LWS (resubmission from 2024) aims to enhance the cybersecurity and resilience of agricultural enterprises in Austria through systematic threat analysis and targeted security strategies. This will make a significant contribution to competitiveness and supply security.
Cyber.LWS is conducting the first sector-specific cybersecurity assessment for Austrian agriculture by systematically transferring existing security concepts and methods from other areas (e.g., the automotive sector) to agricultural use cases and operational structures.
Instead of a generic approach, Cyber.LWS focuses on different types and sizes of operations as well as varying levels of digitization. The goal is to create an agriculture-specific threat database in the ThreatGet tool, in addition to the threat analysis, to enable automated analysis of further systems, even after the project concludes.
The project aims to answer the following questions:
• Which cyber threats are relevant to agriculture and how can attackers proceed?
• Where are the vulnerabilities and what consequences/impacts can arise for operations and supply security?
• What overarching countermeasures (training, regulatory requirements (assessment of relevance of CRA, UN R155, NIS2)) can be implemented to minimize risks and who is responsible for them?
• How can the results be integrated into national programs by political decision-makers?
• What overarching strategies for farmers, manufacturers, and the state, incorporating relevant regulations, can be developed for future security standards in the agricultural sector?
The project is expected to provide sustainable benefits for the following stakeholders:
• Farmers: Scalable preventive measures through low-threshold solutions such as training, awareness programs, and checklists, as well as a focus on basic IT security measures.
• Service providers/manufacturers: Recommendations for hardware and software security requirements that align with

existing strategies (e.g., Cyber Resilience Act, National ICT Security Strategy) and approaches for certification and testing procedures to prevent manipulation and attack scenarios.
• Government organizations: Opportunities to integrate the results into national programs (e.g., funding systems) for long-term and widespread implementation, as well as the use of ThreatGet analyses and project results as a basis for political measures, legal guidelines, and funding content.

Thus, the project strengthens cyber resilience and supply security in Austria.

Following a feedback meeting with the FFG, the following adjustments were made in the resubmission:
• The level of innovation was clarified and the exploitation potentials were specified.
• Planning and method selection were refined, work packages were structured, and resources for vulnerability analysis were expanded.
• Relevant results from previous projects were presented more concretely.
• Resource allocation was adjusted after critical evaluation.
• The value proposition was formulated more clearly.
• Gender balance in the team was improved.

Projektkoordinator

- REPUCO Unternehmensberatung GmbH

Projektpartner

- Raumberg-Gumpenstein Research and Development - Einrichtung mit eigener Rechtspersönlichkeit an der Höheren Bundeslehr- und Forschungsanstalt für Landwirtschaft Raumberg-Gumpenstein
- AIT Austrian Institute of Technology GmbH
- SBA Research gemeinnützige GmbH
- Josephinum Research
- Bundesministerium für Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft