SeRWas

Sichere Resiliente Wasserwirtschaft

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIras Kooperative CS F&E Projekte (KFE CS_2022)	**Status**	laufend
Projektstart	01.12.2023	**Projektende**	28.02.2026
Zeitraum	2023 - 2026	**Projektlaufzeit**	27 Monate
Keywords	Cyber-Resilienz Trinkwasserversorgung Abwasserentsorgung KI CPS IIOT Digitaler Zwilling Cyber-Situationsanalyse Cyber-Sicherheitstraining Gamification		

Projektbeschreibung

Wasserversorgungs- und Abwasserreinigungsanlagen wandeln sich stetig von traditionell physischen Infrastrukturen zu cyber-physischen Systemen (CPS). Die Digitalisierung bringt neue Schwachstellen und Angriffsflächen für Attacken aus dem Cyberraum mit sich. Es gibt eine Zunahme von gemeldeten Cyberangriffen auf Anlagen der Wasserwirtschaft, die zeigen, dass funktionierende Präventivmaßnahmen genauso notwendig sind wie eine frühzeitige Erkennung und Lokalisierung der angegriffenen Systemkomponenten. Klassische Mechanismen zur Erkennung von Cyberangriffen werden zunehmend unwirksamer. Gleichzeitig entstehen jedoch durch den Einsatz neuer Technologien neue Risiken im Bereich Recht und Ethik. Um diese neuen Herausforderungen zu bewältigen, wird SeRWas Forschungsleistungen im Hinblick auf eine umfassende Lösung zur Cyber-Situationsanalyse (Cyber Situational Awareness) für die Wasserwirtschaft durchführen, welche bereits die künftigen rechtlichen, regulatorischen und ethischen Anforderungen mitberücksichtigt. Im Einzelnen wird SeRWas der Wasserwirtschaft helfen,
(1) die Angriffsflächen für Cyberattacken durch Methoden und Tools für detailliertes Assessment und Risikoanalyse zu reduzieren,
(2) der zunehmenden Raffinesse von Cyberangriffen entgegenzuwirken, indem fortschrittliche und robuste Algorithmen als vertrauenswürdige Instrumente der künstlichen Intelligenz (KI) für die frühzeitige und fortlaufende Erkennung von Angriffen und eine bessere Situations- und Risikoeinschätzung entwickelt werden, und
(3) die Anpassung an bewährte Verfahren und die Sensibilisierung auf sich neu entwickelnde Sicherheitsarchitekturen durch zielgruppenspezifisch angepasste innovative Methoden der Wissensvermittlung zu verbessern.

Abstract

Water supply and wastewater treatment plants are steadily transforming from traditional physical infrastructures to cyber-physical systems (CPS). Digitalization brings new vulnerabilities and attack surfaces for attacks from cyberspace. There has been an increase in reported cyberattacks on water management assets, demonstrating that working preventive measures are as necessary as early detection and location of attacked system components. Traditional mechanisms for detecting cyberattacks are becoming increasingly ineffective. At the same time, however, the use of new technologies is creating new

legal and ethical risks.
To address these new challenges, SeRWas will conduct research services towards a comprehensive cyber situational awareness solution for the water industry that already takes into account future legal, regulatory, and ethical requirements. Specifically, SeRWas will help the water industry to
(1) reduce the attack surface for cyberattacks through methods and tools for detailed assessment and risk analysis,
(2) counter the increasing sophistication of cyberattacks by developing advanced and robust algorithms as trusted artificial intelligence (AI) tools for early and ongoing attack detection and better situational and risk assessment; and
(3) improve alignment with best practices and awareness of emerging security architectures through targeted innovative knowledge delivery methods.

Endberichtkurzfassung

Digitale Transformation in der Wasserwirtschaft, Risiken und das Potential für zur Resilienzsteigerung

Für die Sicherheit von IT und OT-Systemen sind, neben umfassender Bewusstseinsbildung für Gefährdungen und Schwachstellen, ein systematisches Risikomanagement und die Umsetzung eines kontinuierlichen Verbesserungsprozesses essentiell, um Anlagen und Personal vor sich laufend ändernden Gefährdungslagen zu schützen. Basierend auf unterschiedlichen Ansätzen zum Risikomanagement in der Cybersecurity wurde ein Konzept ausgewählt, um auf die spezifischen Bedürfnisse des Sektors in Österreich einzugehen, inklusive der Identifikation von kritischen Systemkomponenten, der Rollen-Verteilung von zuständigen Stellen und Verantwortlichen sowie einer einfache Risikobewertung, die unterschiedliche Angriffsvektoren miteinbezieht. White Papers, Leitfäden und aktuelle Forschungsergebnisse, sowie Branchendaten für die Siedlungswasserwirtschaft in Österreich (Referenzen ÖWAV und ÖVGW) lieferten die Ausgangsbasis für eine Roadmap, die es allen Anlagenbetreiber*innen ermöglichen soll, ihre Anlagen systematisch zu erfassen, Schwachstellen zu erkennen und diese je nach Vulnerabilität und Risiko zu beheben.

Digitale Zwillinge im Umfeld der Siedlungswasserwirtschaft

Es wurden bestehende numerische Modelle aus Teilabschnitten des Wasserversorgungssystems sowie Abwasserreinigungsanlagen, implementiert und in EPANet bzw. SIMBA#, eingesetzt, um die Grenzen bei Erstellung, Kalibrierung und Validierung von digitalen Zwillingen in der Siedlungswasserwirtschaft aufzuzeigen und zu diskutieren. Der Fokus beim digitalen Zwilling im Bereich der Wasserversorgungssystems lag in der Lösung von den Herausforderungen der Integration von heterogenen Datensätzen (Prozess und Betriebsdaten, sowie Wetter und Kalenderdaten) und dem Mangel an Smart Meter Daten (das heißt zeitlich und räumlich hochaufgelöster Verbrauchs- bzw. Kund*innendaten) zur hydraulischen Modellierung. Bei der Abwasserreinigungsanlage wurde das unkalibrierte Prozess- und Steuerungsmodell mit 2 Jahren hochauflösender Betriebsdaten verschnitten, um Anomalien zu simulieren und diese schlussendlich in die historischen Prozessdaten zu integrieren. Dies bildete die Ausgangsbasis für das KI-basierte Sicherheitsmanagement unter Verwendung von Anomaliedetektion.

KI-basiertes Sicherheitsmanagement

Zwei neuartige physik-augmentierte Modelle zur Anomalieerkennung wurden entwickelt, die klassische Verfahren wie Isolation Forest, One-Class SVM oder Gaussian Mixture Models deutlich übertreffen. Durch die Integration physikalischer Systemkenntnisse gelingt es diesen Modellen, komplexe Zusammenhänge im Betriebsverhalten technischer Anlagen präziser zu erfassen und mit hoher Trennschärfe zwischen regulären und manipulierten Zuständen zu unterscheiden. Ergänzt wird dieser Ansatz durch zwei komplementäre algorithmische Entwicklungen: Zum einen durch den Hybrid Temporal Differential Consistency Autoencoder, der Momentaufnahmen von Betriebszuständen mit deren zeitlichen Veränderungen kombiniert und so besonders sensitiv auf dynamische Anomalien reagiert. Zum anderen durch Attack-aware Varianten, die gezielt Angriffsdaten in den Trainingsprozess einbeziehen und so die Robustheit gegenüber realitätsnahen Störungsszenarien deutlich erhöhen. Darüber hinaus zeigen die Modelle eine stabile Leistung unter variierenden Rausch- und Parameterbedingungen sowie über unterschiedliche Netzwerktopologien hinweg. Beide Ansätze zeigen eine vergleichbare Performance, die über den aktuellen Stand der Technik hinausgeht. Dies wird unter anderem durch die Auswertung auf dem BATADAL-Datensatz belegt, bei der eine Gesamtbewertung von S?=?0.97 erzielt wurde. Diese Metrik berücksichtigt sowohl die Klassifikationsgüte als auch die zeitliche Verzögerung zwischen dem Beginn eines Angriffs und dem ersten Ausschlag des Detektors.

Gamifizierte Lernkonzepte für Cybersicherheitstrainings in der Siedlungswasserwirtschaft

Für die Wissensvermittlung hinsichtlich möglicher Bedrohungen aus dem Cyberraum wurden vier unterschiedliche Konzepte erarbeitet. Ein Fragenbogen, zur Erhebung des aktuellen Standes der Sicherheitsvorkehrungen im Konnex zu NIS-2 Richtlinie, ermöglicht den Unternehmen eine Abschätzung seines Status diesbezüglich sowie entsprechenden Handlungsbedarf abzuleiten. Zwei unterschiedliche Gamifizierungsansätze, einer in Form einer Mission ein weiterer in Form einer Game-Map, ermöglichen einen spielerischen Ansatz domänenspezifisches Know-how bezüglich Cybersicherheit zu vermitteln. Ein Modul mit dem Schwerpunkt Risikomanagement ermöglicht es den Betreibern von Anlagen in der SWW, dieser mitunter von NIS-2 vorgeschrieben Themenfeld näher zu bringen.

Projektkoordinator

- JOANNEUM RESEARCH Forschungsgesellschaft mbH

Projektpartner

- Holding Graz - Kommunale Dienstleistungen GmbH
- Xylem Water Solutions Deutschland GmbH
- ipcenter.at GmbH
- Technische Universität Graz
- Bundesministerium für Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft