Cyber-Resilienz im Hafen: Innovative IT Architektur sichert die Kommunikation in See- und Binnenhäfen

Forschungsprojekt SecProPort erfolgreich abgeschlossen

Bremen/Bremerhaven, 09.03.2022: *Das vom* Das vom Bundesministerium für Digitales und Verkehr (BMDV) *im Rahmen des Programms „Innovative Hafentechnologien (IHATEC)" geförderte Forschungsprojekt SecProPort zielte drauf ab, skalierbare Sicherheitsarchitekturen für Geschäftsprozesse in deutschen Häfen zu definieren und vereinte die Expertise von insgesamt acht Projektpartnern. Koordiniert durch die dbh Logistics IT AG gehörten zum Projektkonsortium Akteure aus der Hafenwirtschaft – BLG LOGISTICS GROUP AG & Co. KG, Duisburger Hafen AG und Hapag-Lloyd AG – sowie Forschungseinrichtungen – DFKI GmbH, Universität Bremen – und ein Dienstleister im Bereich der Informationssicherheit, die datenschutz cert GmbH. Als Forschungseinrichtung zählte das Institut für Seeverkehrswirtschaft und Logistik (ISL) ebenso zu den Projektpartnern und war maßgeblich am erfolgreichen Projektabschluss beteiligt.*

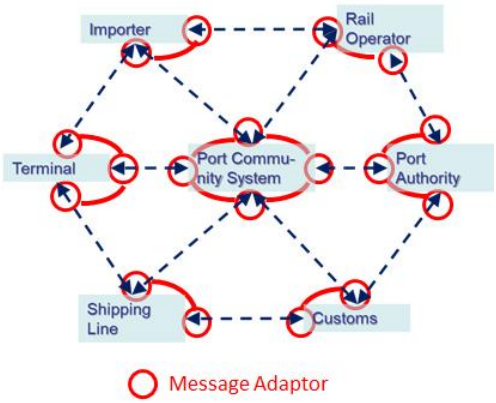
Gemeinsam mit Partnern aus dem gesamten Spektrum des Hafentransports entwickelte das ISL anhand einer Prozess- und Bedrohungsanalyse eine übergreifende Sicherheitsarchitektur für den Kommunikationsverbund im und um den Hafen. Die detaillierte Anforderungsanalyse auf Basis der vier projektbegleitenden Szenarien sowie Evaluation der entwickelten Sicherheitsarchitektur und Dissemination der Projektergebnisse geschah federführend durch das ISL.

Umfangreiche Analysen als Grundlage für die praktische Umsetzung

Die Funktion moderner See- und Binnenhäfen basiert auf elektronisch verfügbaren Informationen, welche die physischen Waren begleiten oder diesen vorauseilen. Alle am Hafentransport beteiligten Akteure (wie z. B. Terminalbetreiber, Reeder, Spediteure, Betreiber von Port-Community-Systemen, Bahn, Hafenbehörden und Zoll) sind hierzu in einem komplexen Hafenkommunikationsverbund miteinander vernetzt und tauschen untereinander Informationen aus. Die Hafenprozesse sind davon abhängig, dass dieser gesamte IT-Kommunikationsverbund reibungslos funktioniert. Selbst, wenn die einzelnen Systeme der Hafenakteure nach dem Stand der Technik abgesichert sind, bedeutet das nicht automatisch, dass der gesamte Hafenkommunikationsverbund im Zusammenspiel sicher ist. Ein Ausfall oder eine Manipulation von Nachrichten an einer Stelle kann zu erheblichen betriebs- und volkswirtschaftlichen Schäden in der Gesamtkette führen. Genau hier setzt SecProPort an: Die beteiligten Partner aus Forschung und Wirtschaft haben ein global abgestimmtes Sicherheitskonzept entwickelt, so dass der Kommunikationsaustausch in einem gesamthaft gesicherten und geschützten Umfeld ablaufen kann.

Hierzu wurde zunächst eine detaillierte Prozessanalyse der vier das Projekt begleitenden Szenarien (Gefahrgutanmeldung über das National Single Window, Container Logistik, XXL-Logistik, die den Transport und die Verschiffung von großen Gütern wie Windturbinen- oder Flugzeugteilen umfasst, und Binnenhafenterminal) durchgeführt. Federführend geschah dies durch Susanne Ficke, verantwortliche Projektleiterin beim ISL Bremen/Bremerhaven und ihrem Team: "*Es wurden systematisch die komplexen Hafenprozesse, Kommunikationsstrukturen und die jeweiligen Sicherheitsanforderungen bei den beteiligten Akteuren analysiert bevor Risikobewertungen und Maßnahmen zur Risikobehandlung am Beispiel des Seehafens Bremerhaven erarbeitet werden konnten.*"

"*Jeder Akteur betreibt in der Regel seine eigenen, mitunter langjährig etablierten Anwendungen, die mit IT-Systemen anderer Partner über dedizierte Schnittstellen verbunden sind. Für die praktische Umsetzbarkeit einer zentralen Sicherheitsarchitektur war es uns wichtig, diese vorhandenen Strukturen zu berücksichtigen*.", erläutert Michael Schröder, Projektmanager beim Projektpartner Hapag Lloyd den SecProPort-Ansatz. Um den Datentransfer zwischen den logistischen Akteuren abzusichern, setzt SecProPort daher auf einen einheitlichen Message Adaptor, der die Systeme der einzelnen Beteiligten effizient ergänzt und sicher miteinander verknüpft.

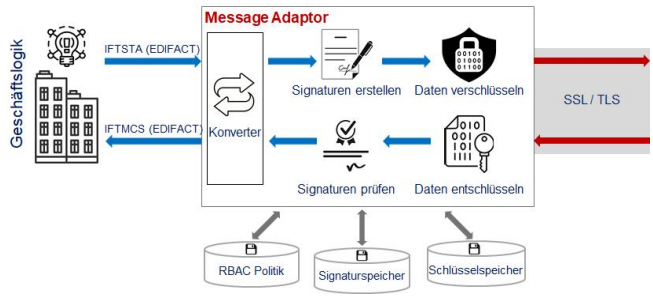


Grafik 1: Message Adaptor als Kommunikationsschnittstelle

Integrität und Vertraulichkeit von Daten im Fokus

Um die Zurechenbarkeit und Manipulationsfreiheit von Daten zu gewährleisten, müssen in der SecProPort-Sicherheitsarchitektur kryptographische Verfahren angewendet werden. Dazu setzt der SecProPort Message Adaptor eine Publik Key Infrastruktur ein. Jeder Akteur erhält von der Zertifizierungsstelle ein eigenes Zertifikat, mit dem ein öffentlicher und privater Schlüssel zur digitalen Signatur sowie Ver- und Entschlüsselung von Nachrichten verbunden ist. Das verhindert die Manipulation von Nachrichten und ermöglicht es, die Echtheit des Absenders zu bestätigen.

Der Sicherheitsarchitektur liegt darüber hinaus eine rollenbasierte Zugriffskontrolle (RBAC - Role Based Access Control) zugrunde. Für jeden Akteur ist detailliert definiert, welche Informationen geschrieben, gelesen oder nicht eingesehen werden dürfen. "*In der Kombination mit kryptographischen Verfahren bietet sich damit sogar die Möglichkeit, dass Daten von beteiligten Akteuren zwar weitergegeben, aber erst vom berechtigten Empfänger der Informationen entschlüsselt werden können*", erklärt Prof. Dr. Dieter Hutter vom Forschungsbereich Cyber-Physical Systems des Deutschen Forschungszentrums für Künstliche Intelligenz (DFKI) die Eigenschaften der entwickelten Sicherheitsarchitektur.



Grafik 2: Der Message Adaptor sorgt für eine einheitliche Absicherung des Datenaustausches im Datenkommunikationsverbund - ohne in bestehende Geschäftslogiken einzugreifen

"*Heutzutage sind nicht nur Sicherheitsmechanismen benötigt, um sich vor Cyberbedrohungen zu schützen, sondern auch eine Resilienzstrategie, um die Geschäftskontinuität auch bei Cybervorfällen zu gewährleisten*", erläutert Konsortialpartner Prof. Dr. Thomas Kemmerich (Universität Bremen). Unter Cyber-Resilienz versteht man die Fähigkeit, sich effektiv auf Cyber-Vorfälle vorzubereiten, diese zu verhindern, zu erkennen, darauf zu reagieren und sich davon zu erholen.
Dementsprechend trägt als weiterer Projektbaustein die Erkennung und konsequente Behandlung von Angriffen zu einer sicheren IT-Infrastruktur im Hafenkommunikationsverbund bei. Das SecProPort-Netz erfüllt Resilienzanforderungen, indem es potenziell mit Schadsoftware befallene oder böswillig agierende Akteure erkennt, die entsprechenden Kommunikationswege einschränkt und gegebenenfalls auf zusätzlich definierte Sicherheitsmechanismen zurückgreift. Zielsetzung ist es, Auswirkungen auf andere Akteure zu minimieren und das betroffene System kontrolliert wieder in einen Normalzustand zu überführen.

Eine Blaupause für andere Kommunikationsverbünde

Im Rahmen des Projektes ist ein Migrationskonzept erstellt worden, das beschreibt, wie die entwickelte Sicherheitsarchitektur nach und nach in einen Produktivbetrieb überführt werden kann. Konzipiert wurde SecProPort dabei ausdrücklich so, dass eine Umsetzung nicht nur im Seehafen, sondern auch für Binnenhäfen oder andere Strukturen möglich ist. Es wurde eine branchenspezifische Prüfgrundlage für kritische Infrastrukturen entwickelt, die mit allen relevanten Interessensgruppen abgestimmt werden kann. Diese erfüllt bereits die Anforderungen des IT-Sicherheitsgesetztes, der DSGVO und der ISO 27001 und kann somit als Vorlage für andere Häfen dienen. Die eingesetzten offenen Datenformate und Plattformtechnologien erleichtern es ebenfalls, die entwickelte Sicherheitsarchitektur für andere Strukturen zu adaptieren. Dennoch stellt Projektkoordinatorin Karin Steffen-Witt heraus: "*Sicherheit in einem Kommunikationsverband kann nur gemeinsam erreicht werden. Sicherheitsregeln müssen von allen Akteuren gemeinsam erarbeitet und vereinbart werden. Dafür müssen sich alle Akteure am Prozess beteiligen und allen die Mechanismen und Handlungsanweisungen transparent zugänglich gemacht werden*."

Weitere Informationen sowie ein Animationsvideo über das Projekt finden Interessierte auf der Projektwebseite: SecProPort

Über das Projekt SecProPort

Für ein außenhandelsorientiertes Land wie Deutschland ist die Funktion moderner See- und Binnenhäfen von existenzieller Bedeutung. Diese basiert zunehmend auf elektronisch verfügbaren Informationen, welche die physischen Warenketten begleiten. Alle am Hafentransport beteiligten Akteure (wie z.B. Terminalbetreiber, Reeder, Spediteure, Betreiber von Hafen-IT, Bahn, Hafenbehörden und Zoll) sind in einem komplexen Hafenkommunikationsverbund (HKV) miteinander vernetzt und tauschen Informationen untereinander aus. Ein Ausfall der Kommunikation kann zu erheblichen betriebs- und volkswirtschaftlichen Schäden führen. Diese Kommunikation wird heute massiv durch Cyberangriffe bedroht. Das Projekt SecProPort zielte drauf ab, eine Sicherheitsarchitektur für den HKV auf Basis einer Prozess- und Bedrohungsanalyse zu entwickeln. Diese Sicherheitsarchitektur sollte Resilienzanforderungen erfüllen, so dass das Gesamtsystem auch im Falle eines Angriffs weiterarbeitet. Aus der Sicherheitsarchitektur wurden Sicherheitsanforderungen für die Anwendungen der einzelnen Hafenakteure abgeleitet und Migrationspläne entwickelt. Zudem wurde bei einzelnen Anwendungspartnern die Sicherheitsarchitektur beispielhaft umgesetzt, um ihre praktische Relevanz nachzuweisen.
Die SecProPort Projektergebnisse flossen in einen Entwurf für einen branchenspezifischen Standard für die Informationssicherheit im Bereich Hafen.

Projektlaufzeit

11/2018 – 12/2021

Gefördert durch:

Bundesministerium für Digitales und Verkehr

aufgrund eines Beschlusses des Deutschen Bundestages

Projektpartner

dbh Logistics IT AG, Bremen
BLG LOGISTICS GROUP AG & Co. KG, Bremen
datenschutz cert GmbH, Bremen
Deutsches Forschungszentrum für Künstliche Intelligenz, Bremen
Duisburger Hafen AG, Duisburg
Hapag-Lloyd AG, Hamburg
ISL Institut für Seeverkehrswirtschaft und Logistik (ISL), Bremen/Bremerhaven
Universität Bremen

Assoziierte Partner

bremenports GmbH & Co. KG, Bremen/Bremerhaven
EUROGATE GmbH & Co. KGaA, KG, Bremen
Niedersachsen Ports GmbH & Co. KG, Oldenburg
JadeWeserPort Realisierungs GmbH & Co. KG, Wilhelmshaven

Über das ISL:
Das ISL - Institut für Seeverkehrswirtschaft und Logistik wurde 1954 in Bremen gegründet. Mit der Verbindung von Tradition und moderner Wissenschaft hat es sich seither als eines der europaweit führenden Institute für maritime Forschung, Beratung und Know-how Transfer mit Schwerpunkten in den Bereichen Maritime Intelligence, Maritime Environment, Maritime Security, Maritime Supply Chains sowie Maritime Digital Innovations etabliert. Mehr unter www.isl.org

Kontakt:

Prof. Dr. Burkhard Lemper
Geschäftsführer (Vorsitz)
Tel.: +49 421 22096 63
E-Mail: lemper@isl.org

Prof. Dr. Frank Arendt
Geschäftsführer
Tel.: + 49 421 22096 17
E-Mail: arendt@isl.org

Susanne Ficke
Projektleiterin
Tel.: +49 471 309838 14
E-Mail: ficke@isl.org

Vivienne Kochanowski
Öffentlichkeitsarbeit
Tel.: +49 421 22096 83
E-Mail: kochanowski@isl.org