Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Verbundprojekt: SecProPort – Skalierbare Sicherheitsarchitekturen für die Geschäftsprozesse in deutschen Häfen

Teilvorhaben ISL: Geschäftsprozesse, Kommunikationsprozesse, ökonomische Auswirkungen

(Förderkennzeichen: 19H18012C)

Individueller Schlussbericht

Leitung: **Dr. Nils Meyer-Larsen (ISL)**

Mitarbeit: **Susanne Ficke (ISL), Rainer Müller (ISL)**

Laufzeit: **01.11.2018 – 31.12.2021**

Datum: **15.04.2022**

Inhaltsverzeichnis

I. Kurzdarstellung

1. Aufgabenstellung

Der Seeverkehr ist von zentraler Bedeutung in der Weltwirtschaft. Hierüber fließen mehr als 90% der interkontinental gehandelten Güter. Damit sind die Häfen für Deutschland essenziell und Voraussetzung für den wirtschaftlichen Erfolg. Die Funktion moderner See- und Binnenhäfen basiert verstärkt auf elektronisch verfügbaren Informationen, die die physischen Warenketten begleiten. Angesichts dieser zunehmenden Digitalisierung wird der Schutz vor Cyberkriminalität in den Häfen immer wichtiger. Ein Ausfall kann zu erheblichen betriebs- und volkswirtschaftlichen Schäden führen.

An der gesamten Transportkette vom Versender zum Empfänger sind zahlreiche Akteure beteiligt. Sie sind in großen Universalhäfen zumeist in komplexen Hafenkommunikationsverbünden (HKV) miteinander vernetzt und tauschen eine große Anzahl von Nachrichten und Information hierüber aus. Sobald diese Informationen von unbefugten Personen verändert, neu oder in falscher Art und Weise in das System eingespielt werden, kann es dazu führen, dass Prozesse im Hafen verzögert werden oder sogar vollständig unmöglich werden. Von einem erfolgreichen Cyberangriff auf den Hafenkommunikationsverbund können alle beteiligten Akteure betroffen sein. Im schlimmsten Fall könnte der Hafen dadurch komplett ausfallen. Die betriebs- und volkswirtschaftlichen Folgen wären erheblich. Es gibt auch Daten, bei denen die Vertraulichkeit sichergestellt werden muss. So ist es denkbar, dass zum Beispiel Informationen über die transportierten Güter oder den Warenverkehr von Unbefugten abgegriffen werden. Das erleichtert den Diebstahl von Waren.

Ziel dieses Verbundprojekts war die Entwicklung einer umfassenden IT-Sicherheitsarchitektur für den Hafenkommunikationsverbund, sodass Cyberangriffe verhindert und im Falle eines erfolgreichen Cyberangriffs die Häfen ihre Funktion weiter ausüben können. Die innovative Architektur soll die verschiedenen Sicherheitsanforderungen der in dem Netzwerk ablaufenden Kommunikationsprozesse unterstützen, diese vor Sabotage schützen und das Ausspionieren von sensiblen Daten durch Dritte verhindern. Die Umsetzung dieses Sicherheitskonzepts sieht vor, dass der Informationsaustauch in einem sicheren geschützten Umfeld abläuft.

Das Teilvorhaben des ISL behandelte schwerpunktmäßig die Aufnahme und Dokumentation der domänenspezifischen Geschäfts- und Kommunikationsprozesse im Umfeld der Hafen-

kommunikation. Dieses beinhaltete auch die Aufnahme der Sicherheitsanforderungen der Prozesse und der verarbeiteten Daten. Darüber hinaus evaluierte das ISL die Projektergebnisse im Sinne einer Kosten-Nutzen-Analyse des konzipierten HKV. Dem ISL oblag die Leitung der Arbeitspakete „AP 1 Anforderungsanalyse“ und „AP 7 Dissemination und Evaluation“. Diese Arbeitspakete bildeten damit auch die Arbeitsschwerpunkte des ISL in diesem Projekt. Das ISL brachte hierzu seine umfangreichen Kontakte zu Unternehmen und Verbänden der maritimen Wirtschaft ein. Darüber hinaus verfügt das ISL aus diversen früheren Projekten über umfangreiche Erfahrungen und Expertise im Bereich Dissemination, die im Projekt zum Einsatz kamen.

2. Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Das SecProPort-Konsortium bestand aus insgesamt acht Partnern aus Forschungseinrichtungen und der Praxis. Neben dem Institut für Seeverkehrswirtschaft und Logistik brachten die Praxispartner

- dbh Logistics IT AG — Betreiber Hafenkommunikationsverbund (HKV)
- Hapag-Lloyd AG — Reeder
- BLG Logistics GROUP — Logistiker
- Duisburger Hafen AG — Hafenbetreiber

ihre Kenntnisse und Erfahrungen in die Projektarbeit ein. Sie repräsentierten einzelne Akteure des Hafenkommunikationsverbundes. Auf der anderen Seite konnten

- datenschutz cert GmbH
- Deutsches Forschungszentrum für Künstliche Intelligenz GmbH (DFKI)
- Universität Bremen

ihre ausgewiesene Kompetenz hinsichtlich organisatorischer, methodischer und technischer Sicherheit von IT-Systemen in das erfolgreiche Projektergebnis einbringen. Als eines der führenden europäischen maritimen Forschungs- und Beratungsinstitute agierte das ISL mit dem Hintergrund langjähriger Kooperationen mit den Beteiligten im Hafenumfeld, ausgewiesener

Kontakte zur Hafenwirtschaft, exzellenter Kenntnisse auf dem Gebiet Hafen- und Terminalabläufe sowie der Koordination des Vorgängerprojekts PortSec als Schnittstelle zwischen den Anwendern im Hafenumfeld und den IT-Partnern.

Das Konsortium bildete somit einen ausgewogenen Mix aus den relevanten Akteuren im Bereich des Hafentransports sowie Forschungspartnern mit Erfahrung auf dem Gebiet der IT-Sicherheit. Der Projektverlauf zeigte, dass diese Konstellation eine sehr gute Basis für die erfolgreiche Bearbeitung der umfangreichen Aufgabenstellung darstellte.

3. Planung und Ablauf des Vorhabens

Die Arbeiten für das Projekt SecProPort wurden am 01. November 2018 aufgenommen. Die geplante Laufzeit des Vorhabens betrug drei Jahre, sodass die Planung den Abschluss der Projektarbeiten zum 31. Oktober 2021 vorsah. Die Einschränkungen, die durch die seit Anfang 2020 aufgetretene COVID-19 Pandemie verursacht wurden, führten allerdings zu zeitlichen Verzögerungen in der Bearbeitung der einzelnen Arbeitspakete. Dieses wurde dem Projektträger von den Projektpartnern auf den Konsortialtreffen im Dezember 2020 und Juni 2021 sowie in den Zwischenberichten für den Berichtszeitraum 2020 angezeigt. Im August 2021 beantragten alle Partner daher eine kostenneutrale Verlängerung der Projektlaufzeit um zwei Monate. Das ISL beantragte weiterhin eine Mittelumwidmung in Höhe von 11.300 Euro aus den Positionen 0838 Reisekosten und 0813 Material zur Position 0837 Personalkosten. Der Grund hierfür war die nur noch sehr eingeschränkte Möglichkeit, die interessierte Öffentlichkeit im Rahmen von Veranstaltungen und Workshops über das Projektziel und den aktuellen Projektverlauf zu berichten. Das ISL hatte die Idee, durch die Erstellung und Verbreitung von Animationsfilmen, die über die Webseite heruntergeladen werden können, über die Projektergebnisse zu berichten und damit den Arbeitsumfang und den Personalaufwand für die Bearbeitung des „AP 7 Dissemination“ zu erhöhen. Die Genehmigung hierzu wurde durch den Projektträger erteilt.

Nach einer Laufzeit von drei Jahren und zwei Monaten wurde das SecProPort-Teilvorhaben „Geschäftsprozesse, Kommunikationsprozesse, ökonomische Auswirkungen“ des ISL am 31. Dezember 2021 erfolgreich abgeschlossen.

Nachfolgende Grafik zeigt den Zeit- und Arbeitsplan des Gesamtprojekts, der die einzelnen Arbeitspakete mit ihren Teilaufgaben und den verantwortlichen Leitern sowie die zeitliche Einbettung in die Gesamtprojektlaufzeit beinhaltet.

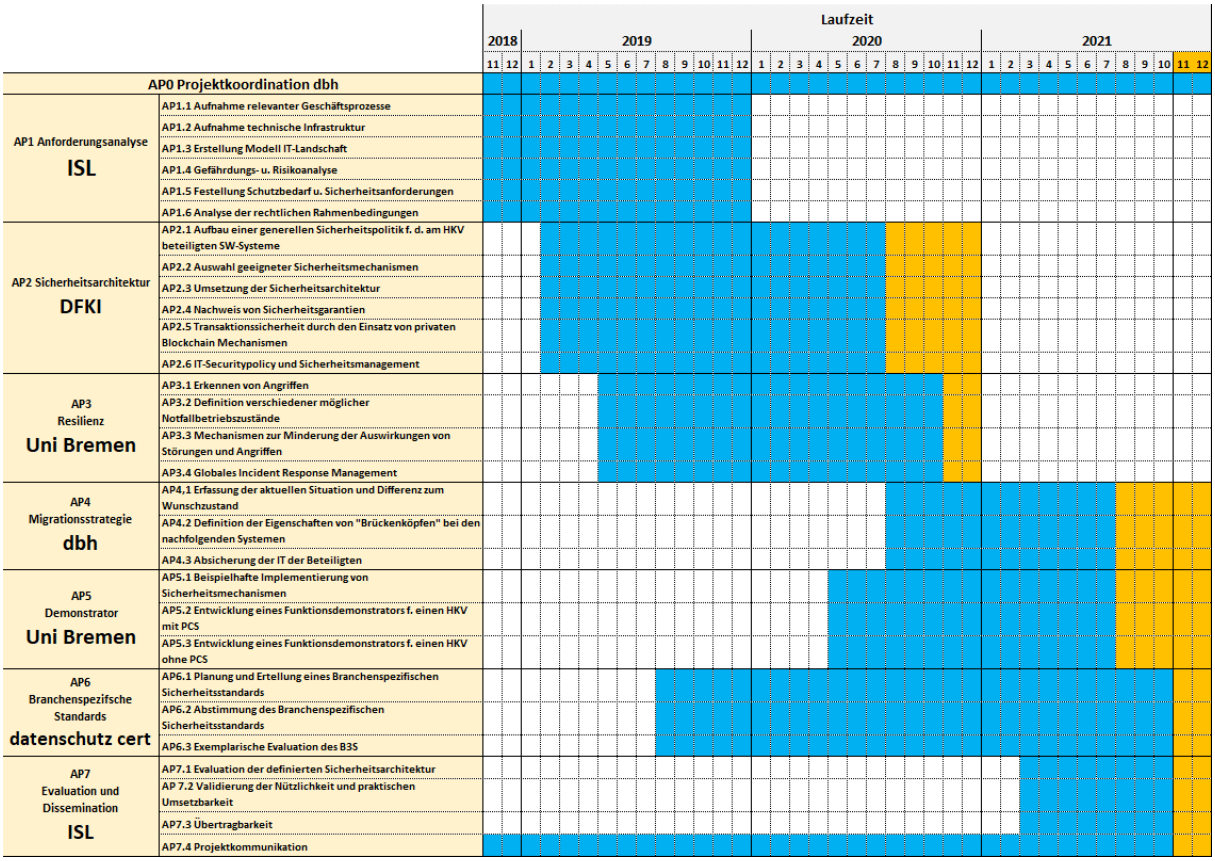

Abbildung 1 Projektplan (nach kostenneutraler Verlängerung)

4. Wissenschaftlicher und technischer Stand

Das ISL führt seit vielen Jahren Forschungs- und Entwicklungsprojekte mit Bezug zur Cyber-Security in der maritimen Logistik durch (sowohl auf regionaler, nationaler als auch EU-Ebene). Daher verfügte das ISL bereits bei Projektstart über exzellente Kontakte und Kooperationen mit allen Beteiligten im Hafenumfeld, die im Rahmen dieses Projekts zielbringend eingesetzt werden konnten und durch die erfolgreiche Bearbeitung dieses Projekts auch noch weiter ausgebaut wurden.

Das ISL strebt an, die im Rahmen dieses Projekts erarbeiteten Ergebnisse und Erkenntnisse auch in anderen zukünftigen Projekten im Hafenumfeld einzusetzen. Hierzu gehört auch die Technologie der Prozessaufnahme mit dem Standardformat Business Process Model and Notation (BPMN), die für die Analyse der Geschäftsprozesse der analysierten Praxisszenarien verwendet wurde und sich im Projektverlauf als äußerst geeignet erwies, um die hohe Komplexität und Detailtiefe der Prozessabläufe darzustellen.

Ferner sollen die Bedrohungsszenarien, die Vorgehensweise zur Ermittlung einer Kosten-Nutzen-Analyse und die Formalisierung der Prozessabläufe inkl. deren Übertragung in zukünftigen Projekten eingesetzt und weiterentwickelt werden.

Das ISL schätzt die Erkenntnisse aus diesem Projekt als Expertise mit hohem Verwertungspotential für die Untersuchung von weiteren Hafentelematiksystemen ein.

5. Zusammenarbeit mit anderen Stellen

Im Rahmen des SecProPort-Projektes wurde seitens des ISL Kontakt zu verschiedenen relevanten Organisationen aufgenommen, um über das Projekt und seine Ziele zu informieren und ggf. Kooperationen anzubahnen. Zu nennen sind hier unter anderem:

- Maritimes Cluster Norddeutschland (MCN)
- Deutsches Zentrum für Luft- und Raumfahrt - Institut für den Schutz maritimer Infrastrukturen, Bremerhaven
- 13. Oldenburger Versicherungstag: Cyber-Versicherungen
- Verein Hanseatischer Transportversicherer e.V. (VHT) - Expertenkreis Informationssicherheit für Reedereien
- Nautischer Verein Bremerhaven

Außerdem erfolgte ein bilateraler Erfahrungsaustausch mit den in die Projektarbeit eingebundenen assoziierten Partnern, wobei hier insbesondere die bremenports GmbH & Co. KG zu nennen ist, die für das Hafenmanagement der Häfen Bremerhaven und Bremen zuständig ist.

II. Eingehende Darstellung

1. Verwendung der Zuwendung und erzielte Ergebnisse

Das Teilvorhaben des ISL behandelte schwerpunktmäßig die Aufnahme und Dokumentation der domänenspezifischen Geschäfts- und Kommunikationsprozesse im Umfeld der Hafenkommunikation (AP 1 Anforderungsanalyse). Dieses beinhaltete auch die Aufnahme der Sicherheitsanforderungen der Prozesse und der verarbeiteten Daten. Im Rahmen des Arbeitspakets 7 evaluierte das ISL die Projektergebnisse im Sinne einer Kosten-Nutzen-Analyse des konzipierten HKV.

Für die Außendarstellung der Projektinhalte hat das ISL eine Projektwebseite (www.secproport.de) aufgebaut und betrieben. Auch die Entwicklung von Flyern und Roll-Up lag in der Verantwortung des ISL. Das ISL erstellte außerdem zwei Animationsfilme, in denen die Projektinhalte in Video und Audio vermittelt werden. Ein Download hierfür steht auf der Webseite zur Verfügung (www.secproport.de/de/animationsfilme).

- SecProPort Projektkurzbeschreibung (03:17 Minuten)
- SecProPort Projektergebnis (08:20 Minuten)

Im Folgenden werden die Ergebnisse der Arbeitspakete beschrieben, in die das ISL schwerpunktmäßig eingebunden war.

AP 1 Anforderungsanalyse

In diesem Arbeitspaket fungierte das ISL als Arbeitspaketleiter und koordinierte alle hier zu bearbeitenden Aufgaben der beteiligten Projektpartner.

Die Gesamtaufgabe untergliederte sich in folgende sechs Teilarbeitspakete:

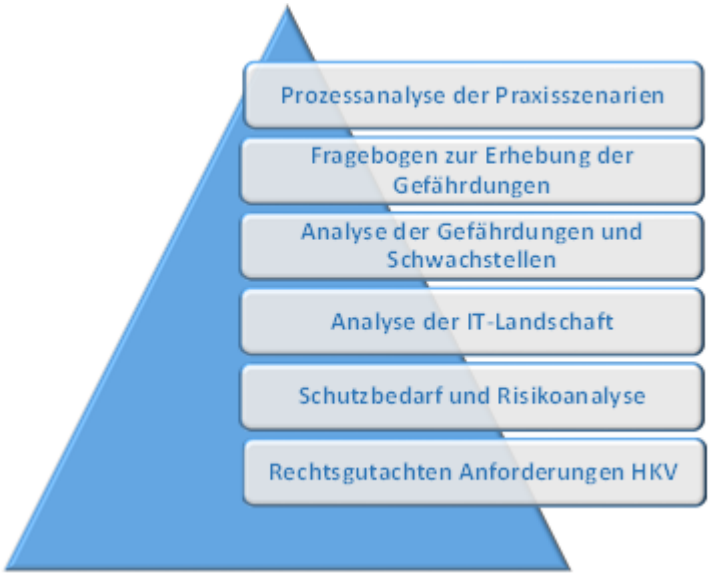

Abbildung 2 Struktur „AP 1 Anforderungsanalyse“

Prozessanalyse der Praxisszenarien

Im Rahmen der Anforderungsanalyse wurde eine detaillierte Prozessanalyse der vier das Projekt begleitenden Szenarien durchgeführt. Jedes der Szenarien ist einem der im Konsortium eingebundenen Praxispartner zugeordnet:

- **S1: Gefahrgutanmeldung**
  über das National Single Window dbh Logistics IT AG
  Seit dem 01. Juni 2015 müssen Schiffsanläufe in deutschen Häfen verpflichtend elektronisch über das Zentrale Meldeportal des Bundes gemeldet werden. Dies betrifft das Einlaufen und das Auslaufen von Schiffen in einen bzw. aus einem Hafen in Deutschland sowie die Transitreise eines Schiffes durch den Nord-Ostsee-Kanal. Die Meldeverpflichteten eines einkommenden oder ausgehenden Seeschiffes übermitteln die Daten, wie die Schiffsanmeldung (Hafenamt), das Besatzungsverzeichnis (Bundespolizei) oder die Gefahrgutanmeldung (Hafenamt). Diese Informationen werden an das NSW-Kernsystem übermittelt. Das National Single Window stellt sicher, dass jeder Empfänger, wie Bundespolizei, Hafenamt und Seegesundheitsbehörde, genau die Informationen bekommt, die er braucht. Die Meldung kann über die Webanwendung Advantage National Single Window (ANSW) der dbh durchgeführt werden.

- **S2: Container-Logistik Hapag-Lloyd AG**
  In diesem Szenario wird die Container-Logistik untersucht, d.h. der Weg des Containers von der Auftragsvergabe bis zum Empfänger. Hierbei erfolgt eine Unterteilung in Export- und Importrichtung, d.h. Containerzulauf zum Terminal (Export) und Containerablauf vom Terminal (Import).
- **S3: XXL-Logistik BLG Logistics GROUP AG & Co. KG**
  Mit diesem Szenario wird der Umschlag von großen und schweren Waren (XXL) nachgebildet. Ein Kunde der BLG ist ein weltweit agierender Hersteller von Wellpappkartonagen, der über die Bremischen Häfen sogenannte Kraftliner aus Skandinavien importiert. Die bis zu 3,5t schweren Rollen werden von der BLG zunächst eingelagert und auf Abruf zumeist per LKW zu den weiterverarbeitenden Wellpappfabriken transportiert. Gleichzeitig exportiert der Kunde über die Bremischen Häfen das sogenannte Fluting (das für die „Welle“ der Wellpappe verwendete Altpapier) nach England. Diese Rollen werden in der Regel per Waggon in den Bremischen Häfen angeliefert, eingelagert und auf Abruf aufs Schiff verladen.
- **S4: Binnenhafenterminal Duisburger Hafen AG**
  Mit Einbindung dieses Szenarios wurden auch die Abläufe eines Binnenhafenterminals in die Projektuntersuchung betrachtet.

Zunächst wurden systematisch für die einzelnen Szenarien die relevanten komplexen Geschäfts- und Kommunikationsprozesse für den Hafenbetrieb wie z.B. Export, Import, National Single Window und Transshipment aufgenommen und dokumentiert. Hierbei wurden auch die verschiedenen Rollen und beteiligten Akteure identifiziert, die an der Ausführung der einzelnen Prozessschritte beteiligt sind. Die Dokumentation der Prozesse erfolgte in BPMN-Diagrammen. Darüber hinaus wurden Informationen über die IT-Infrastruktur der einzelnen Systeme des Hafenverbundes (inkl. relevanter Übertragungsprotokolle wie z.B. HTTP(S), SFTP und OFTP) ermittelt und die vorhandenen Software-Systeme der einzelnen Akteure sowie Schnittstellen zu den IT-Systemen der weiteren Hafenakteure aufgenommen. Es wurden zahlreiche Workshops bei den Praxispartnern BLG Logistics Group, dbh, Hapag-Lloyd sowie dem Binnenhafen Duisburg durchgeführt und die Abläufe, Akteure und deren Rollen sowie Daten und

Vertrauensverhältnisse der einzelnen Rollen/Akteure zueinander aufgenommen. Dazu gehörte auch die Aufnahme von Umfang, Art und Struktur der eingesetzten Kommunikationsmittel, d.h. Schnittstellen, Protokolle und Nachrichtenstrukturen.

Für jedes Szenario erfolgte die Prozessbeschreibung in Form eines detaillierten BPMN-Modells, das aus mehreren Diagrammen besteht. Zur Darstellung der Prozessabläufe wurde die Freeware-Anwendung Bizagi BPMN Modeler verwendet. Hiermit werden die Prozesse in dem als Business Process Model and Notation (BPMN) bekannten Standardformat graphisch abgebildet und dokumentiert. Die zahlreichen erstellten Diagramme beinhalten eine detaillierte Darstellung der Abfolge der Aktivitäten und Ereignisse sowie der für die Umsetzung eines Prozesses erforderlichen Informationsflüsse. Die Vorteile von BPMN liegen darin, dass eine Darstellung in hoher Komplexität und großer Detailtiefe möglich ist. Dieses hat sich als großer Vorteil für die Bearbeitung der weiteren Arbeitspakete erwiesen.

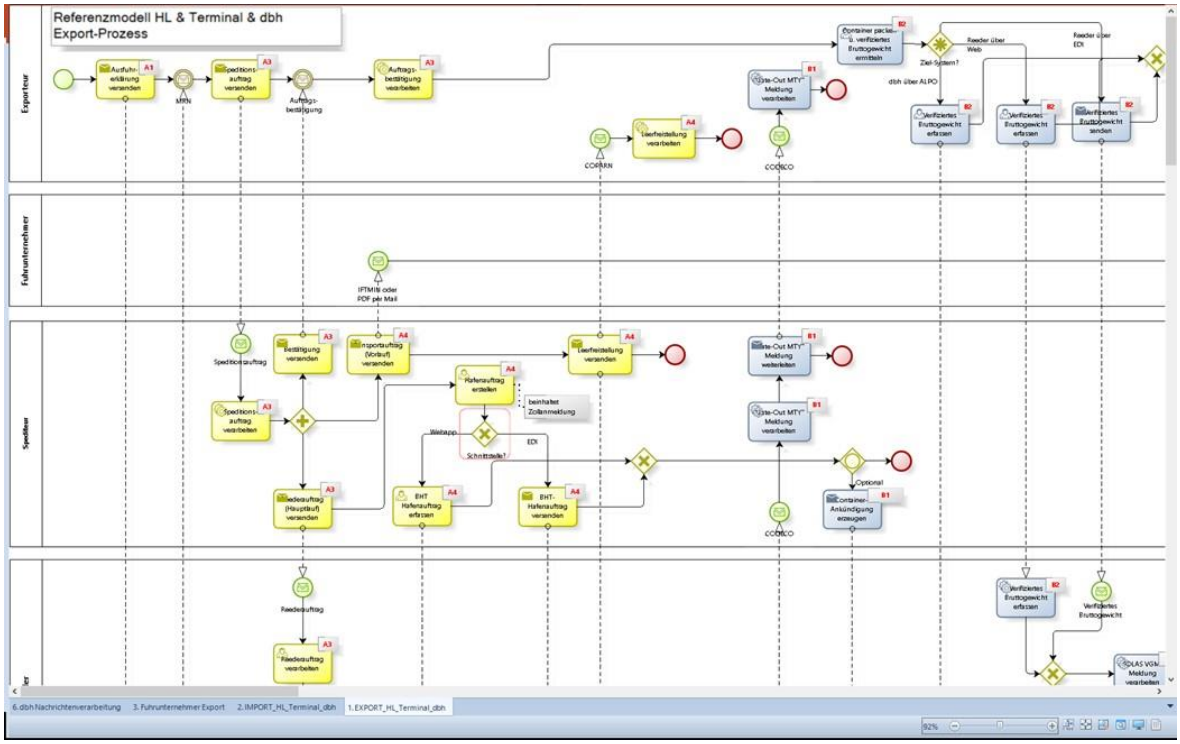

Abbildung 3 Beispiel Auszug BPMN-Diagramm „Export_HL_Terminals_dbh“ aus dem BPMN-Modell „S2 Container-Logistik“

Um auch ein Verständnis der Abläufe in den einzelnen Szenarien in etwas weniger Detailtiefe geben zu können, hat sich das Projektteam dazu entschlossen, zusätzlich für jedes Szenario

eine Prozessdarstellung in ablaufender Form zu erstellen. Hierfür wurde Powerpoint mit seinen Animationsmöglichkeiten verwendet.

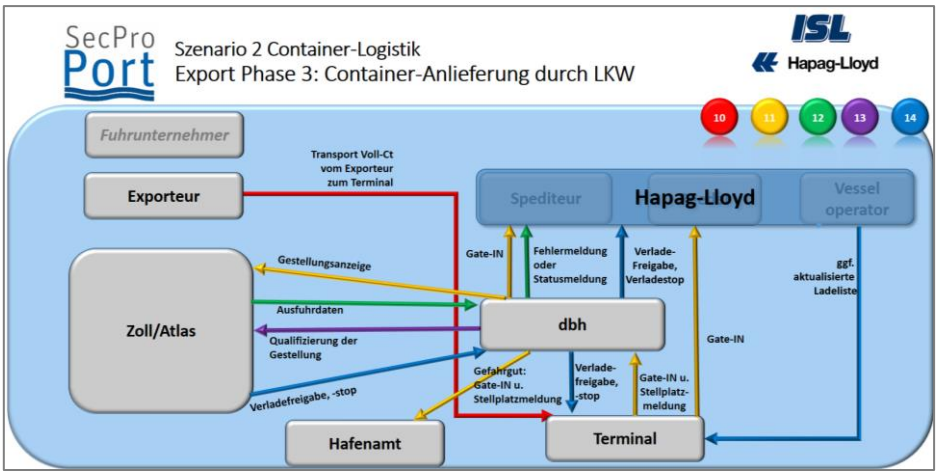

Abbildung 4 Powerpoint/Animation: Szenario 2/Teilszenario Container-Anlieferung durch LKW

Die entwickelten komplexen Prozessmodelle bildeten die Grundlage für alle weiteren Arbeiten im Projekt.

Fragebogen zur Erhebung und Analyse der Gefährdungen und Schwachstellen

Auf Basis der entstandenen Prozessaufnahmen wurden für die einzelnen beteiligten Praxispartner individuelle Fragebögen entwickelt. Diese wurden dazu genutzt, die jeweiligen Gefährdungen, Risiken, Eintrittswahrscheinlichkeiten und Anforderungen zu ermitteln. Hierbei erfolgte die Unterteilung in lokale, d.h. unmittelbare, Gefahren und globale Gefahren mit weiterreichenden Folgen. Das Risiko der Eintrittswahrscheinlichkeit wurde in fünf Kategorien von „unwahrscheinlich“ (weniger als einmal in 10 Jahren zu erwarten) bis „sehr wahrscheinlich“ (einmal monatlich oder häufiger zu erwarten) unterteilt. Außerdem wurde die Relevanz bezüglich der Wahrscheinlichkeit des Eintritts und dem Grad der Auswirkung abgefragt. Die hier ermittelten Gefährdungen waren die Grundlage für die anschließende Risikoanalyse und die Ermittlung der Schutzbedarfe der betroffenen Systeme.

Analyse der IT-Landschaft/Schutzbedarf und Risikoanalyse

In die Beschreibung der IT-Landschaft flossen die Informationen aus einer Vielzahl von Experteninterviews mit den eingebundenen Praxispartnern, Erfahrungsaustausch mit Hafenbehörden und weiteren Unternehmen aus dem Hafenumfeld sowie den Ergebnissen aus der Prozessanalyse ein. Hierfür wurden dann typische Gefährdungen und Schwachstellen analysiert.

Im nächsten Schritt folgte die Ermittlung des konkreten Risikos und des Schutzbedarfs der einzelnen Assets. Für die Bewertung des Risikos eines Teilprozesses wurde die jeweilige Eintrittswahrscheinlichkeit und Auswirkung einbezogen und somit der Schutzbedarf ermittelt. Basis waren die vorliegenden Antworten aus der Fragebogenumfrage bei den Praxispartnern.

Abschließend wurden Maßnahmen zur Risikobehandlung erarbeitet. Hierbei wurde die Risikominderung, die Risikoakzeptanz, der Risikotransfer sowie die Risikovermeidung betrachtet.

Rechtsgutachten "Anforderungen Hafenkommunikationsverbund (HKV)"

Parallel wurde vom Projektpartner datenschutz cert ein fast 40-seitiges Rechtsgutachten erstellt, in dem die Gesetzeslage hinsichtlich möglicher Anforderungen an die einzelnen Akteure des Hafenverbunds zum Thema Cyber-Sicherheit geprüft wurde. Neben dem IT-Sicherheitsgesetz umfasste die Analyse auch die Datenschutzanforderungen aus der Datenschutzgrundverordnung (DSGVO).

AP 7 Evaluation und Dissemination

In diesem Arbeitspaket fungierte das ISL als Arbeitspaketleiter und koordinierte die Aufgaben der Projektpartner erfolgreich.

Evaluation

Die Arbeiten im Bereich der Evaluation bezogen sich auf die Erstellung einer exemplarischen Kosten-Nutzen-Analyse, die den betriebswirtschaftlichen bzw. den volkswirtschaftlichen Nutzen des Einsatzes der entwickelten Sicherheitsarchitektur den zu erwartenden Kosten gegenüberstellt. Dieses erfolgte exemplarisch, da eine detaillierte Kostenanalyse über alle Beteiligten des HKVs den Rahmen dieses Projekts gesprengt hätte.

Außerdem wurde untersucht, ob die relevanten Faktoren des Konzepts der Sicherheitsarchitektur und des erarbeiteten branchenspezifischen Standards aufeinander abgestimmt sind.

Des Weiteren wurde eine Evaluation der Sicherheitsarchitektur und des Rahmenwerks für Cyber-Resilienz durchgeführt.

Abschließend erfolgte die Betrachtung der Umsetzbarkeit und Übertragbarkeit des entwickelten Sicherheitsarchitekturkonzepts.

Kosten-Nutzen-Analyse

Für die Kosten-Nutzen-Analyse wurden die Kosten für die Implementierung der in SecProPort entwickelten Konzepte grob abgeschätzt. Der Nutzen für die Beteiligten definiert sich durch die implementierte Sicherheitsarchitektur, die Angriffe verhindert und durch das Rahmenwerk für Cyber-Resilienz, das Angriffe frühzeitig erkennt. Bei dieser Analyse wurden betriebs- und volkswirtschaftliche Aspekte betrachtet. So kann ein Ausfall des HKV für einen Betrieb u.a. einen zeitlichen Mehraufwand, Ertragsverluste und Verlust der Reputation bedeuten. Für die Volkswirtschaft wiederum kann es u.a. zu Steuerausfällen und Verlust von Arbeitsplätzen kommen.

Zur Bewertung der Amortisation der Implementierung der im Rahmen dieses Projekts entwickelten Konzepte wurde exemplarisch die Vorgehensweise dargestellt. Hierbei wurden zwei Szenarien betrachtet:

- kurzfristiger Ausfall des HKV über 6 Stunden
- langfristiger Ausfall des HKV über 2 Wochen.

Zur Bewertung der Amortisation müssen die Unternehmen die Kosten für die Implementation der Konzepte den möglichen Schäden gegenüberstellen. Hierzu ist es u.a. auch entscheidend, die Abhängigkeiten der Akteure in einem HKV zu beachten. Hierzu wurde folgende Matrix entwickelt:

Ausfall von / Auswirkung auf	Terminalbetreiber	Reeder	Schiffsmakler	Spediteure	Bahnoperateure	Hafenbahn	Zoll	Hafenbehörden	PCS
Terminalbetreiber		hoch	gering	gering	mittel	hoch	hoch	hoch	hoch
Reeder	hoch		gering	gering	mittel	mittel	hoch	hoch	hoch
Schiffsmakler	mittel	mittel		gering	gering	mittel	mittel	hoch	hoch
Spediteure	hoch	mittel	gering		mittel	hoch	mittel	hoch	hoch
Bahnoperateure	hoch	mittel	gering	gering		hoch	mittel	hoch	hoch
Hafenbahn	hoch	mittel	gering	gering	hoch		mittel	hoch	hoch
Zoll	hoch	mittel	gering	gering	gering	gering		hoch	hoch
Hafenbehörden	mittel	mittel	gering	gering	gering	gering	mittel		hoch
PCS	mittel	mittel	gering	gering	gering	gering	hoch	hoch	

Abbildung 5 Matrix der Abhängigkeiten der Akteure bei Störungen

Zusammenhang Sicherheitsarchitektur und Branchenspezifischer Standard

Im Rahmen der Evaluation der Sicherheitsarchitektur und des branchenspezifischen Standards wurde untersucht, in welchem Umfang die Implementierung der Sicherheitsarchitektur die Anforderung des Standards erfüllt.

Der Prüfstandard bzw. der Branchenspezifische Sicherheitsstandard umfasst viele Aspekte, welche auf die normativen Anforderungen der ISO/IEC 27001, dem IT-Sicherheitskatalog oder dem §8a BSIG aufbauen. Durch die Implementierung der Sicherheitsarchitektur werden einige der Anforderungen automatisch miterfüllt. Maßgeblich betroffen ist hiervon das Zugriffs- und Zugangsrechte-Management, jedoch auch die zwingend notwendige PKI-Infrastruktur. Eine Implementierung der Sicherheitsarchitektur hat demnach zur Folge, dass die Umsetzung der Prüfgrundlage wesentlich, zumindest aus IT-Security-Sicht, erleichtert wird.

Evaluation der Sicherheitsarchitektur und Bewertung des Rahmenwerks für Cyber-Resilienz

Das in AP 2 entwickelte Konzept der Sicherheitsarchitektur wurde in Bezug auf die gesetzten Ziele kritisch evaluiert. Hierbei wurde die Architektur hinsichtlich der Wirkung auf verschiedene Kriterien hin untersucht. Neben den etablierten Grundwerten der Informationssicherheit, Verfügbarkeit, Integrität und Vertraulichkeit wurden auch weitere wichtige Kriterien untersucht, welche die Sicherheitsarchitektur für eine praktische Umsetzung erfüllen sollte. Hierzu zählen Funktionssicherheit, Verlässlichkeit, Datensicherheit, Verbindlichkeit und Authentizität. Außerdem flossen in die Beurteilung der Datenschutz, Performance, Benutzbarkeit, Umsetzbarkeit

und auch die Zukunftsfähigkeit ein. Das Ergebnis der Evaluation zeigt, dass die entwickelte Sicherheitsarchitektur viele geeignete Maßnahmen beinhaltet, die die Sicherheit im Hafenkommunikationsverbund deutlich verbessert.

Auch das Rahmenwerk für Cyber-Resilienz wurde nach primären und sekundären Evaluationskriterien bewertet. Hierzu gehörten die Risikobewertung, Angriffsvermeidung und –erkennung, Reaktion auf Angriffe und Wiederherstellung nach Angriffen sowie als sekundäre Kriterien die Implementierung des Rahmenwerks in den HKV und die Darstellung der Limitierungen des Rahmenwerks.

Als Ergebnis der Evaluation kann festgestellt werden, dass die im Rahmen des Projekts realisierte Sicherheitspolitik (Sicherheitsarchitektur und Rahmenwerk der Cyber-Resilienz) geeignet ist, das angestrebte Ziel der Erhöhung der Sicherheit zu unterstützen.

Umsetzbarkeit

Das in SecProPort erarbeitete Migrationskonzept beschreibt als Best Practice Handbuch die durchzuführenden Maßnahmen für die Migration. Dieses gilt sowohl für Seehäfen als auch für Binnenhäfen. Für die Umsetzbarkeit der in SecProPort entwickelten Konzepte sind organisatorische und technische Umsetzungsvoraussetzungen zu berücksichtigen. Die Umsetzung der Konzepte sollte schrittweise im Rahmen einer Migration erfolgen. Für die organisatorische Migration sollte zunächst ein Entscheidungsgremium gegründet, die Kommunikationsverbindungen der beteiligten Partner analysiert und die Migrationsschritte abgestimmt werden. Anschließend sollte ein zentrales Berechtigungskonzept (Access-Control-Matrix) definiert und eine Zertifizierungsstelle identifiziert werden. Im Bereich der technischen Migration erfolgte die Implementation eines Message-Adaptors, der die zu transportierenden Nachrichten in einen gemeinsamen Standard überführt und mit Hilfe von kryptografischen Verfahren einzelne Attribute absichert. Hierzu muss der Message-Adaptor Signaturen erstellen, prüfen und verwalten können. Außerdem muss die Semantik der verwendeten Attribute definiert und für die Access-Control-Matrix die verwendeten Rollen zu Akteuren zugeordnet werden. Des Weiteren muss eine Schlüsselverwaltung implementiert und im Message-Adaptor die Nachrichten in das entsprechende Format übersetzt werden.

Übertragbarkeit der Sicherheitsarchitektur

Die Analyse der verschiedenen Szenarien hat gezeigt, dass die Sicherheitsarchitektur auf andere Kommunikationsstrukturen übertragbar ist, die ähnliche Anforderungen und eine ähnliche

Komplexität aufweisen wie der Hafenkommunikationsverbund. Hierzu zählen maßgeblich die Anforderungen an die Sicherheit, die Anzahl an Nachrichtentypen sowie die Anzahl und die Komplexität der Zusammenarbeit der Partner im Verbund.

Dissemination

Im Rahmen des Arbeitsbereichs Dissemination wurde eine Projekt-Homepage entwickelt und über die gut dreijährige Projektlaufzeit gepflegt. Außerdem wurden ein Flyer und ein Rollup für die Außendarstellung gestaltet. In den ersten 15 Projektmonaten konnte das Projektkonsortium auf zahlreichen Veranstaltungen über das Projekt und die bisherigen Zwischenergebnisse berichten wie in Kapitel 6 detailliert dargestellt. Aufgrund der sich durch das Corona-Virus ergebenen Einschränkungen spätestens seit April 2020 war dieses so leider nicht mehr möglich. Aus diesem Grund entschloss sich das Konsortium, mit den Einsatz von Animationsfilmen, die über die Webseite heruntergeladen werden können, die Öffentlichkeit über den Projektinhalt zu informieren.

Webseite: www.secproport.de

2. Wichtigste Positionen des zahlenmäßigen Nachweises

Im Projekt sind im Wesentlichen Kosten für Personal und Reisen angefallen. Im Verwendungsnachweis sind diese Kosten detailliert dargestellt.

Die Personalkosten (Position 0837) wurden entsprechend der Projektskizze bzw. des Projektantrags für die Bearbeitung der einzelnen Arbeitspakete verwendet. Der ursprünglich höher dimensionierte Posten „0838 Reisekosten“ ist aufgrund der durch die Corona-Pandemie verursachten Reisebeschränkungen weniger stark in Anspruch genommen worden.

Das ISL leitete das Arbeitspaket „AP 7 Evaluation und Dissemination der Projektergebnisse“, wozu das Teilpaket „AP 7.4 Projektkommunikation“ zählt. Ein Schwerpunkt der hier zu leistenden Arbeiten bezog sich auf die Kommunikation von Projektergebnissen nach außen. Das ISL hat zwei Animationsfilme erstellt, die über den Projektinhalt informieren und über die Webseite heruntergeladen werden können. Die Idee hierzu entstand erst während der Projektlaufzeit, da aufgrund der sich durch das Corona-Virus ergebenen Einschränkungen die Öffentlichkeitsarbeit in Form von Präsenzveranstaltungen nicht möglich war. Hierfür waren höhere Personalressourcen erforderlich, als für das AP 7 ursprünglich veranschlagt. Das ISL hat daher im April

2021 einen Antrag auf Mittelumwidmung gestellt. Insgesamt wurden 11.300 € aus den Positionen „0838 Reisekosten“ (9.950 €) und „0813 Material“ (1.350 €) zu der Position „0837 Personalkosten“ umgewidmet.

3. Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die Bedrohung von Wirtschaftsunternehmen generell und somit auch der Hafenwirtschaft durch Cyberkriminalität nimmt weiter zu[1]. IT-Sicherheit wird auch in Zukunft ein wichtiges Thema sein. Eine Vielzahl von Meldungen bezüglich aktueller Sicherheitslücken und neuer Gefährdungen zeigen die akute – und noch zunehmende – Bedeutung der Thematik für die maritime Wirtschaft. Daher ist es von großer Wichtigkeit, das Thema weiter zu erforschen und neue, innovative Ansätze zur Absicherung entsprechender EDV-Systeme zu entwickeln und somit auf immer neue Angriffsstrategien durch Cyberkriminelle zu reagieren.

Im Rahmen des SecProPort-Projekts konnte erfolgreich die interdisziplinäre Zusammenarbeit der Projektpartner unter Beweis gestellt werden. Dies spiegelt sich aus Sicht des ISL insbesondere in der Bündelung branchenübergreifender Kompetenzen im Anforderungsmanagement (Ableitung von Anforderungen aus Nutzerprofilen) und der Dissemination (Etablierung und Pflege der Projektsichtbarkeit) wider. Die Sichtbarkeit des SecProPort-Konsortiums und dieser Fortschritte konnte etabliert und über die Projektlaufzeit kontinuierlich ausgebaut werden.

Alle geschilderten Aufgaben waren notwendig und angemessen, um die Ziele des ISL-Teilvorhabens und des Gesamtvorhabens erreichen zu können.

4. Voraussichtlicher Nutzen und Verwertbarkeit des Ergebnisses

Die im Rahmen von SecProPort gewonnenen neuen Kenntnisse, insbesondere hinsichtlich Anforderungen der involvierten Industriepartner, flossen unter Berücksichtigung der Vertraulichkeit in die wissenschaftliche Expertise des ISL ein und können in der Zukunft zur Erarbeitung von wissenschaftlichen Strategien zur Lösung bestehender Probleme und zur Optimie-

[1] Vgl. Deutsche Verkehrs-Zeitung (DVZ) 05.07.2021; „Cyberkriminalität: Die Bedrohung wächst“; https://www.dvz.de/rubriken/management-recht/detail/news/die-bedrohung-aus-dem-netz-wird-groesser.html, Abruf 01.04.2022

rung von Prozessen dienen. Diese Erkenntnisse werden als Expertise mit hohem Verwertungspotenzial für die Bearbeitung weiterer Projekte im Bereich Cyber-Security für die maritime Industrie eingeschätzt.

Um die wissenschaftliche Anschlussfähigkeit des Projektes zu gewährleisten, wird das ISL auch in Zukunft anstreben, Synergien mit anderen einschlägigen Forschungsprojekten zu erschließen. Durch bestehende und zukünftige Kooperationen des ISL mit Unternehmen und Verbänden der maritimen Wirtschaft können diese Strategien dann im Rahmen der anwendungsnahen Forschung des ISL in die Praxis umgesetzt werden.

Die Verbundpartner sind sich einig, die gemeinsame Arbeit auch zukünftig fortzuführen. Die Kooperation bietet eine gute Möglichkeit, Unterstützungsleistungen der Hafenwirtschaft als Gruppe anbieten zu können, die kein Partner allein leisten könnte. Wo es sinnvoll ist, wird auch im wissenschaftlichen Bereich die Zusammenarbeit mit den anderen SecProPort-Partnern angestrebt.

Das ISL wird seinen Namen im Bereich Cyber-Security in der maritimen Branche festigen und ausbauen. Ergebnisse und Vorgehensweisen werden auch in die Hochschullehre einfließen. An der Hochschule Bremerhaven ist das SecProPort-Poster seit Sommer 2021 im Gebäude T ausgehängt, wo der Masterstudiengang ISSM (Integrated Safety & Security Management) beheimatet ist:

Abbildung 6 SecProPort-Poster in der Hochschule Bremerhaven

5. Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen

Ein Vertreter der Ashdod Port Company – einer der wichtigsten Häfen Israels -, hat im letzten Quartal der Projektlaufzeit Kontakt zum Projektkonsortium aufgenommen. Im Rahmen einer Videokonferenz kam es zum Informationsaustausch. Ashdod Ports wird sehr oft angegriffen und ist sehr an Digitalisierung und der damit verbundenen Cyber-Security interessiert. Hierzu wurden rund 30 Start-Ups gegründet, die an Innovationen für den Port arbeiten. Das Start-Up EasySec Solutions beschäftigt sich dabei intensiv mit der Cyber-Security und IIOT (Industrial Internet of Things). Hier ist man mit der Entwicklung des Produkts ThinGuard beschäftigt, das die Zugriffsrechte der IIOT-Devices und der User regelt.

Als weiteres Projekt im Rahmen des Förderprogramms IHATEC – Schwerpunkt Sicherheit – beschäftigt sich HITS-Moni (Harbour – IT – Security – Monitoring) mit der IT-Sicherheit im Hafenumfeld (Projektlaufzeit März 2019 – Februar 2022). Dieses Projekt hat seinen Schwerpunkt in der Erkennung von Cyberangriffen und der Verringerung der Anzahl unbedeutender Sicherheitswarnungen. Im Gegensatz zu SecProPort, das das Untersuchungsfeld gesamtheitlich betrachtet, liegt im Projekt HITS-Moni der Schwerpunkt in der Resilienzberachtung des Systems.

6. Erfolgte oder geplante Veröffentlichungen der Ergebnisse

Im Rahmen von SecProPort war das ISL an folgenden Veröffentlichungen beteiligt:

Datum	Name	Artikel	Link
11/2018	Nordsee-Zeitung, Bremerhaven	Neue Software soll Sicherheitslücken aufspüren	
01/2019	Internationales Verkehrswesen	SecProPort - Häfen vor Caberangriffen schützen	
07/2019	Institut für Seeverkehrswirtschaft und Logistik	Thesenpapier: Millionenschäden in Häfen durch Cyberangriffe	https://www.isl.org/de/news/neues-thesenpapier-isl-millionenschaeden-haefen-cyberangriffe
09/2019	Sonntagsjournal, Bremerhaven	Wenn Hacker den Hafen kapern	
10/2019	THB - Tägliche Hafenbericht	Hafen-IT vor Cyberangriffen schützen	
10/2019	JOT: Journal of Object Technology	Modeling and Validating Role-Based Authorization Policies for a Port Communication System with UML and OCL	https://www.jot.fm/contents/issue_2020_03/article8.html
11/2019	Sonntagsjournal, Bremerhaven	Digitaler Angriff auf den Umschlag	
08/2020	Transport Research Arena (TRA) 2020	Advances of Cybersecurity in Maritime Port Operations	
02/2021	Proceedings of the 7th International Conference on Information Systems Security and Privacy – ICISSP	Ontology-based Cybersecurity and Resilience Framework	https://www.scitepress.org/Link.aspx?doi=10.5220/0010233604580466
Ausgabe 2021	SUT: Schiffahrt Hafen Bahn und Technik	SUT Serie: Förderprogramm für innovative Hafentechnologien (IHATEC); IT-Sicherheitsarchitekturen	
04/2021	PIANC Working Group 208: MarCom WG Report no. 208-2021	Planning for Automation of Container Terminals	https://www.isl.org/index.php/de/news/neue-publikation-planning-automation-container-terminals-veroeffentlicht
06/2021	IEEE International Conference on Communications Workshops, ICC	A Framework For Intelligent DDoS Attack Detection and Response using SIEM and Ontology	https://doi.org/10.1109/ICCWorkshops50388.2021.9473869
10/2021	Logistics Pilot	Sicherer Hafen	
10/2021	Logistics Pilot	Sicherer Hafen	
10/2021	Proceedings of the first European Workshop on Maritime Systems Resilience and Security (MARESEC 2021)	Where are my containers?	https://zenodo.org/record/5604449
10/2021	Proceedings of the first European Workshop on Maritime Systems Resilience and Security (MARESEC 2021)	Threat Modeling Knowledge for the Maritime Community	https://zenodo.org/record/5604234
11/2021	IAME Conference	Towards a secure and reliable IT-ecosystem in seaports	https://arxiv.org/abs/2111.13436

Abbildung 7 Übersicht Veröffentlichungen zum Projekt SecProPort

Die folgende Tabelle enthält die Veranstaltungen, auf denen SecProPort durch das ISL vertreten wurde:

Datum	Veranstaltungsort	Veranstaltungsname	Titel	Vortragender
15.11.2018	Bremerhaven	Science goes Public	Vortag: Häfen Cybersecure!	Nils Meyer-Larsen/ISL
04.-07.06.2019	München	Messe transport logistic	Messestand: Digitalisierung und Cyber-Sicherheitsbedrohungen in der Transport- und Logistikbranche	Karin Steffen-Witt/dbh, Nils Meyer-Larsen/ISL
10.09.2019	Bremerhaven	Nautischer Verein zu Bremerhaven	Vortag: Cybersecurity in der Maritimen Logistik	Nils Meyer-Larsen/ISL
11.09.2019	Oldenburg	13. Oldenburger Versicherungstag: Cyber-Versicherungen	Erfahrungsaustausch	Nils Meyer-Larsen/ISL
18.09.2019	Berlin	IHATEC Statusseminar	Interview: Projektinhalt SecProPort	Karin Steffen-Witt/dbh weitere Teilnehmer: Nils Meyer-Larsen/ISL Thomas Kemmerich/Uni Bremen
26.-27.09.2019	Hamburg	Hamburg International Conference of Logistics (HICL)	Vortag: Artificial Intelligence and Digital Transformation - Risk Management	Nils Meyer-Larsen/ISL
23-24.10.2019	Bremerhaven	International Symposium on Digital Platforms for Maritime Safety and Security Applications	Messestand: Vorstellung Projektinhalt SecProPort	Nils Meyer-Larsen/ISL
30.10.2019	Bremerhaven	Maritimes Cluster Norddeutschland (MCN)	Vortrag: Cyber Security for Maritime Infrastructure	Nils Meyer-Larsen/ISL
19.11.2019	Bremerhaven	Verein Hanseatischer Transportversicherer e.V. (VHT) Expertenkreis Informationssicherheit für Reedereien	Erfahrungsaustausch	Nils Meyer-Larsen/ISL
25.11.2019	Berlin	BMVI Arbeitskreis Sicherheit in der Logistik	Erfahrungsaustausch	Nils Meyer-Larsen/ISL
25.11.2021	Rotterdam (online)	IAME 2021 (International Association of Maritime Economists Conference 2021)	Vortag: Towards a secure and reliable IT-ecosystem in seaports	Rainer Müller/ISL

Abbildung 8 Übersicht Vorträge und Messeteilnahmen des ISL zum Projekt SecProPort