Abschlussbericht

Verbundprojekt SecProPort

19H18012D

datenschutz cert GmbH

Leitung Dr. Sönke Maseberg

Mitarbeit Aiko Czembor, Thomas Heinemann, Tim-Niklas Koch, Klaus-Werner-Schröder, Michael Eschen, Jan Schirrmacher

Laufzeit	01.11.2018 – 31.12.2021
Datum	07.02.2022

Inhaltsverzeichnis

1 Kurzdarstellung

1.1 Aufgabenstellung

Ziel des Vorhabens war es, eine Sicherheitsarchitektur für den Hafenkommunikationsverbund systematisch auf Basis einer Prozess- und Bedrohungsanalyse zu entwickeln. Diese Sicherheitsarchitektur erfüllt Resilienzanforderungen, so dass das Gesamtsystem auch im Falle eines Angriffs weiterarbeitet. Aus der Sicherheitsarchitektur wurden anschließend Sicherheitsanforderungen für die Anwendungen der einzelnen Hafenakteure abgeleitet und Migrationspläne entwickelt. Zusammen mit einzelnen Anwendungspartnern wurde dann die Sicherheitsarchitektur beispielhaft in Demonstratoren umgesetzt, um ihre praktische Relevanz nachzuweisen. Die Projektergebnisse flossen zudem in einen Entwurf eines branchenspezifischen Standards für die Informationssicherheit im Bereich Hafen ein.

Die datenschutz cert GmbH hat in dem Projekt die Rolle des erfahrenden Informationssicherheits-Dienstleisters bzw. der akkreditierten Zertifizierungsstelle übernommen. Maßgebliche Aufgaben waren die Erstellung einer ausführlichen Risikoanalyse-Methodik zur Ermittlung lokaler und globaler Risiken im Hafenumfeld, der Unterstützung jeglicher Art hinsichtlich Fragen zum Bereich der Informationssicherheit, der Durchführung von Schwachstellenscans bei den Partnern sowie der Erstellung einer Prüfgrundlage zur Durchführung von KRITIS-Audits.

1.2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Die datenschutz cert GmbH waren bereits am Vorgängerprojekt PortSec ausführlich beteiligt. Hier wurde erkannt wie wichtig das Thema ist und somit durch SecProPort weitergeführt. Die Wichtigkeit wird vor allem durch die dauerhafte Risikolage und den stetigen Angriffen gegenüber Hafenbetreibern bzw. Logistikunternehmen (z.B. Maersk) deutlich. Eine Weiterführung mit Partnern aus der Praxis (Hapag-Lloyd, BLG, duisport) war dadurch mehr als sinnvoll.

Intern gab es in Laufe des Projektes mehrere Personalveränderungen, die den Ablauf des Projektes jedoch nicht gestört haben.

Die Covid19-Pandemie hat die datenschutz cert GmbH, wie alle anderen Unternehmen, hinsichtlich der Reisetätigkeiten eingeschränkt. Durch die vielseitigen Remote-Lösungen und Videokonferenz-Tools hatte dies jedoch keinen Einfluss auf den Erfolg des Projektes.

1.3 Planung und Ablauf des Vorhabens

Die Arbeiten am Projekt wurden innerhalb einer 36-monatigen Laufzeit von November 2018 bis Oktober 2021 geplant. Der Durchführung wurde dabei ein Arbeitsplan zugrunde gelegt, welcher 7 Arbeitspakete vorsieht.

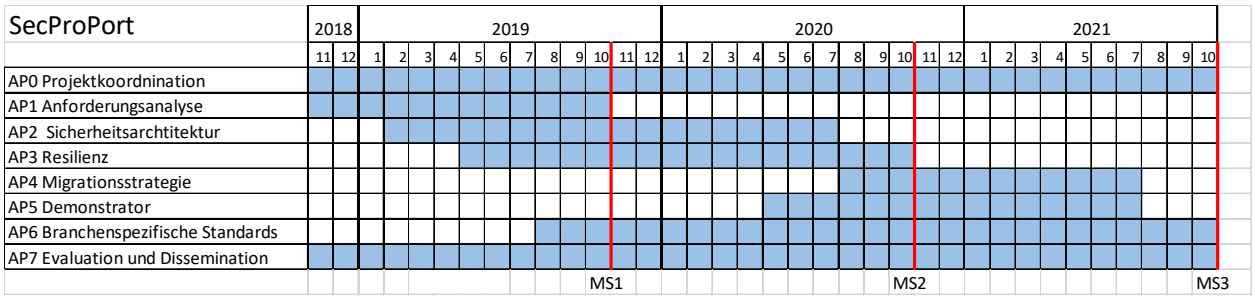


Abb. Ursprünglicher Projektplan

Bedingt durch die Covid19-Pandemie, den damit verbundenen Kontaktbeschränkungen und bei den Konsortialpartnern verhängten Dienstreiseverboten war es uns seit April 2020 nicht möglich, Präsenzmeetings zur Projektarbeit durchzuführen. Es kam zu Verzögerungen in den verschiedenen Arbeitspakten, die sich auf die anschließenden Arbeitspakete übertrugen, so dass im Juni 2021 ein Antrag auf kostenneutrale Projektverlängerung um 2 Monate gestellt wurde

Für die restliche Projektlaufzeit wurde ein neuer Projektplan aufgestellt:

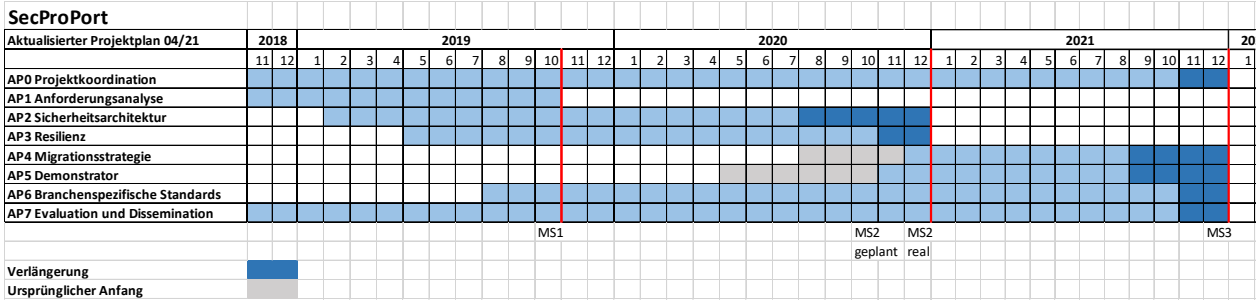


Abb. Angepasster Projektplan

1.4 Wissenschaftlicher und technischer Stand, an den angeknüpft wurde

Für das Projekt SecProPort wurden die wissenschaftlichen Ergebnisse aus dem Vorgängerprojekt PortSec verwendet und hier inhaltlich angeknüpft. Für das Projekt waren u.a. viele Gesetzestexte, wie dem BSIG, der KRITIS-Verordnung, dem IT-Sicherheitsgesetz 2.0, der DSGVO und weitere Hafenspezifische Gesetze.

1.5 Zusammenarbeit mit anderen Stellen

Im Rahmen der Projektlaufzeit wurde von mehreren externen Unternehmen Interesse am Projekt geäußert. So konnte z.B. mit easysec Solutions und dem Port of Aschdod die Prüfgrundlage in gemeinsamer Arbeit überarbeitet werden. Außerdem gab es Projekt-Telkos mit Kühne & Nagel sowie HLAG.

2 Verwendung der Zuwendung

2.1 Erzielte Ergebnisse und Gegenüberstellung der vorgegebenen Ziele

Die Gesamtergebnisse des Projektes sind dem Gesamtabschlussbericht zu entnehmen. Die datenschutz cert GmbH hatte den größten Workload in den Arbeitspaketen 1 und 6 sowie mehrere Projektmonate verteilt auf die anderen Pakete.

Die Ergebnisse des Arbeitspaketes 1 können grundsätzlich in drei Bereiche eingeteilt werden: Unterstützungsleistungen, Risikoanalyse, Rechtsgutachten. Im Detail ist hiermit gemeint, dass die dsc zum einen in AP 1.1 und AP 1.2 die anderen Forschungspartner maßgeblich durch Expertise unterstützt hat. Auf der anderen Seite wurde im Rahmen von AP 1.6 ein detailliertes Rechtsgutachten sowie im Rahmen von AP 1.3 und AP 1.4 eine ausführliche Risikoanalyse erstellt, die für die Arbeitspakete 2, 3 und 6 von wichtiger Bedeutung sind. Die gemeinsam gesammelten Ergebnisse aus AP 1.1 und AP 1.2 konnte die dsc wiederrum für die Risikoanalyse verwenden.

AP 1.1: Wie zuvor beschrieben, hat die dsc in AP 1.1 die Praxispartner vor allem durch die langjährige Erfahrung im Bereich der IT- und Informationssicherheit unterstützen können, die Prozessmodellierung so zu modellieren, dass auf dem ersten Blick mögliche Schwachstellen und Angriffspunkte identifiziert werden konnte. Im Detail wurden in diesem Arbeitspaket vier konkrete Szenarien in Zusammenarbeit mit den Praxispartner erstellt: Szenario 1 (Gefahrgutanmeldung über das National Single Window), Szenario 2 (Container Logistik), Szenario 3 (XXL-Logistik), Szenario 4 (Binnenhafenterminal). Für alle vier Szenarien wurde vom Projektteam eine detaillierte Prozessbeschreibung erarbeitet. Dabei hat die dsc maßgeblich darauf geachtet, dass bei den Prozessen deutlich wird, welche Daten und wie diese jeweils übermittelt werden. Dies war vor allem für das datenschutzrechtliche Gutachten, als auch für die exemplarische Modell-IT-Landschaft (AP 1.3) notwendig.

AP 1.2: Die Arbeitspakete AP 1.1 und AP 1.2 stehen in direkter Beziehung zu einander. Während AP 1.1 vielmehr die eigentliche Modellierung der Prozesse betrachtet, wurde bei AP 1.2 vielmehr auf die Art, den Umfang und die Struktur der Kommunikationsmittel in den jeweiligen Prozessen geschaut. Die dsc hat in AP 1.2 maßgeblich an der Ermittlung der Kommunikationswege, der Protokolle und Nachrichtenstrukturen mitgewirkt. Im Detail wurden hier sowohl explizite Assets (z. B. IT-Systeme,

Netzwerkkomponenten etc.), als auch konkrete Nachrichtenformate (z.B. ftp oder sftp) und spezifische Nachrichtenformate (COPARN, AUA etc.) ermittelt und einer ersten Schutzbedarfsanalyse unterzogen. Am Ende von AP 1.1 und AP 1.2 konnten für alle Szenarien die Prozessbeschreibungen, bestehend aus der Beschreibung der einzelnen Prozessschritte (Excel), eine vereinfachte animierte Darstellung der Abläufe (PowerPoint) sowie ein detailliertes BPMN Prozessmodell (Bizagi BPNM Modeler), fertiggestellt werden.

Die Durchführung von Penetrationstests war im Rahmen des Projektes nur bedingt möglich. Zwar wurde ein Penetrationstest bei der dbh durchgeführt, welcher für das Projekt auch sinnvoll war, jedoch wurde von weiteren Penetrationstests (z.B. bei Hapag-Lloyd) abgesehen. Dies lag maßgeblich auch daran, dass die Penetrationstests im Rahmen des Projektes durch Jan Schirrmacher durchgeführt wurden (zertifizierter Penetrationstester) und dieser das Unternehmen in Laufe des Projektes verlassen hat. Hier sei angemerkt, dass dieser immer noch auf einen geringen Stundensatz bei der datenschutz cert GmbH angestellt ist und kleinere Tätigkeiten für uns durchführt (u.a. Penetrationstests).

Im Rahmen seiner neuen Tätigkeit bei bremenports (assoziierter Partner des Projektes) konnte die Thematik jedoch auf eine andere Art und Weise fortgeführt werden. So bietet bremenports Schwachstellenscans für Hafeninfrastrukturen an, um diesen Sicherheitslücken in deren Systeme zu präsentieren. Aiko Czembor, welcher sich in einem stetigen Austausch mit Jan Schirrmacher befindet, konnte sich von der Weiterführung dieser Thematik überzeugen.

AP 1.3: Im Rahmen des AP 1.3 wurde ein exemplarisches Modell einer IT-Landschaft im Hafenumfeld erschaffen. Dabei lag der Fokus weniger auf der Erstellung eines Schaubildes bzw. einer visuellen Darstellung des Modelles (es wurde jedoch trotzdem ein Schauspiel mit geringer inhaltlicher Tiefe erstellt), sondern vielmehr um die Analyse der typischen Kommunikationsstrecken und Verbindungen zwischen den einzelnen Akteuren (z.B. Reeder, Spediteur, Terminalbetreiber etc.) und Systemen (OSIS, ALPO, BHT etc.). Anhand der Analyse konnten typischen Gefährdungen und Schwachstellen herausgefiltert werden. Grundlage für die Analyse waren mehrere Interviews mit den Praxispartnern (z.B. BLG, Hapag-Lloyd), ein Erfahrungsaustausch mit bremenports und dem ISL, die Ergebnisse aus AP 1.1, AP 1.2 und AP 1.4 sowie die Ergebnisse aus dem Vorgänger-Forschungsprojekt PortSec-2. Modellhaft und ohne die Angabe der komplexen Übertragungsprotokolle sieht das Schaubild wie folgt aus:

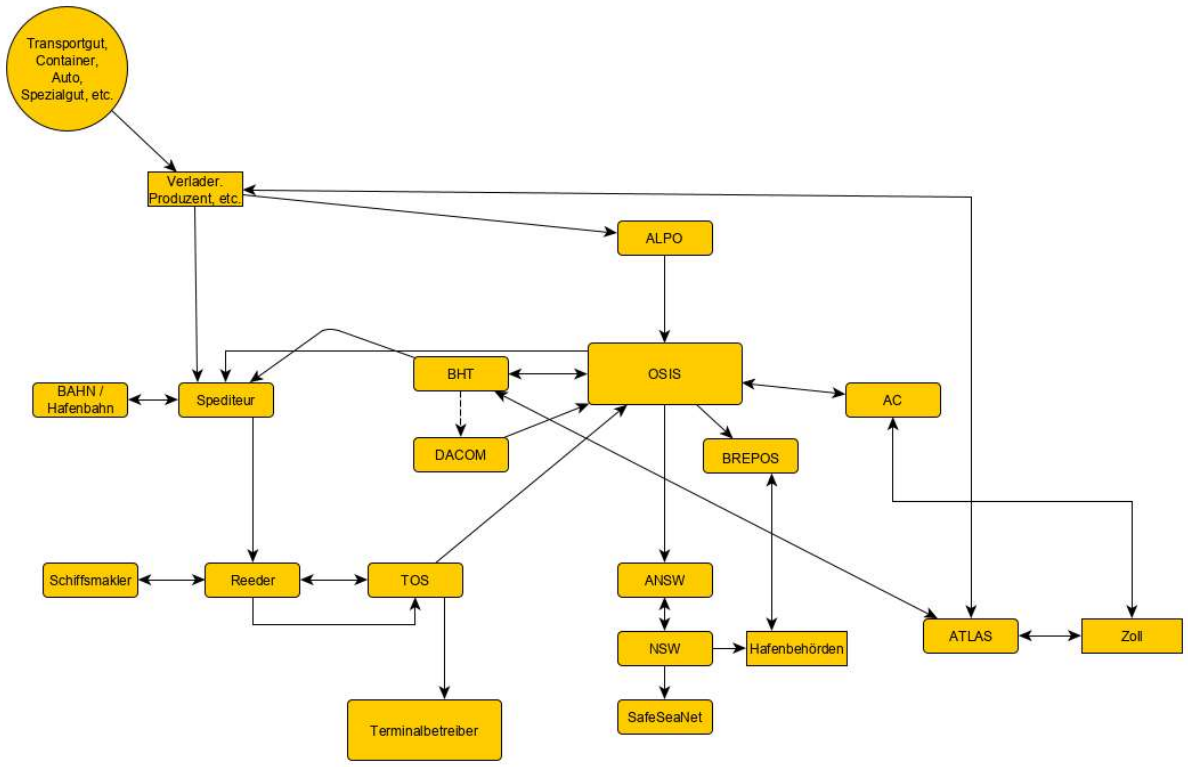


Abbildung IT-Modell Hafenumfeld

Durch die Analyse der IT-Landschaft konnten typische Gefährdungen aufgedeckt werden. Die Gefährdungen lassen sich grundsätzlich in zwei Kategorien, den lokalen und den elementaren Gefährdungen unterscheiden. Die elementaren Gefährdungen orientieren sich in den Vorgaben des BSI (IT-Grundschutz-Kompendium). Dazu gehören nachfolgende 21 Gefährdungskategorien:

- Hacking und Manipulation
- Terroristische Akte (Physisch mit Wirkung auf die IT oder direkt IT bezogen)
- Naturgefahren mit Wirkung auf die IT
- Identitätsmissbrauch (Phishing, Skimming, Zertifikatsfälschung)
- Missbrauch (Innentäter)
- Abhängigkeiten von Dienstleistern und Herstellern (Ausfall für IT-Betrieb erforderlicher externer Dienstleister, unberechtigter Zugriff, versteckte Funktionen in Hard- und Software)
- Unbefugter Zugriff
- Manipulation, Diebstahl, Verlust, Zerstörung von IT oder IT-relevanten Anlagen und Anlagenteilen
- Schadprogramme

- Social Engineering
- Gezielte Störung/Verhinderung von Diensten (DDoS, gezielte Systemabstürze)
- Advanced Persistent Threat (APT)
- Beschädigung oder Zerstörung verfahrenstechnischer Komponenten, Ausrüstungen und Systeme
- Ausfall von Basisinfrastrukturen mit direktem Bezug zur IT (Sekundäreffekte, z. B. Strom und TK)
- Organisatorische Mängel
- Technische Schwachstellen in Software, Firmware und Hardware
- Technisches Versagen von IT-Systemen, Anwendungen oder Netzen (sowie Verlust von gespeicherten Daten)
- Menschliche Fehlhandlungen, menschliches Versagen
- Infrastrukturelle Mängel (baulich, Versorgung mit Strom etc.)
- Verwendung ungeeigneter Netze/Kommunikationsverbindungen, sonstige Schwächen in der Kommunikationsarchitektur
- Verkopplung von Diensten (Beeinträchtigung eines Dienstes durch Störung anderer Dienste)

Die lokalen Gefährdungen ergeben sich maßgeblich aus den, durch das dfki und dem ISL erstellten Fragebogen, der an die Praxispartner verteilt wurde. Die dsc hat die Ergebnisse des Fragebogens gesammelt. Insgesamt konnte hierdurch ca. 50 lokale Gefährdungen zusammengetragen werden. Nach Zusammenführung ähnlicher Gefährdungen (de facto Duplikate), beläuft sich die Anzahl der Gefährdungen final auf 31. Alle Gefährdungen wurden in einer Excel-Tabelle aufgelistet und entsprechenden Akteuren im Hafenumfeld zugeordnet. Die weiterführende Erstellung der eigentlichen Risikoanalyse bzw. des Risikomodells erfolgte zwar simultan, kann jedoch AP 1.4 konkreter zugeordnet werden.

AP 1.4: In AP 1.4 wurden die Ergebnisse aus AP 1.1, 1.2, 1.3 sowie AP 1.5 zu einer konkreten Risikoanalyse zusammengefügt. Zunächst wurde hierfür ein eigenes Risikomodell erschaffen, welches an die ISO/IEC 27005 oder auch in Teilen an den BSI-Standard 200-3 aufweist angelehnt ist. Das bedeutet, dass in dieser Risikobetrachtung die Assets im Mittelpunkt stehen, der Schutzbedarf dessen ermittelt, das Risiko ausgehend von der Eintrittswahrscheinlichkeit berechnet und die Risikobehandlung in den Stufen Risikominderung, Risikoakzeptanz oder Risikotransfer eingeteilt wird

Zunächst wurde definiert, welche Eintrittswahrscheinlichkeiten es geben soll. Demnach gibt es fünf Eintrittskategorien, von unwahrscheinlich (weniger als einmal in zehn Jahren) bis sehr wahrscheinlich

(einmal monatlich oder häufiger). Jede Kategorie wurde mit alternativen Hilfestellen ergänzt. Beispielsweise benötigt es multiples Fachwissen und maßgeschneidertes Equipment seitens des Angreifers, damit ein Risiko mit der Eintrittswahrscheinlichkeit „Unwahrscheinlich“ eintreffen kann.

Im nächsten Schritt wurden die Assets einer Schutzbedarfsfeststellung unterzogen. Insgesamt konnten 13 maßgebliche relevante Assets (z.B. BHT, OSIS, eStore, eCargo etc.) einer Schutzbedarfsfeststellung unterzogen werden. Diese Bewertung erfolgte in gemeinsamer Arbeit mit den jeweiligen Asset-Owner. Für die Bewertung wurde jeweils analysiert, welche Auswirkung die Verfügbarkeit, die Integrität und die Vertraulichkeit auf die Sicherheit/Gesundheit, Umweltschäden, Reputation, finanzielle Schäden, und Versorgungssicherheit hat. Eine Klassifizierung erfolgt in den Kategorien normal (1), hoch (2) und sehr hoch (3). Der Schutzbedarf des einzelnen Assets ergibt sich folglich aus der Addition der maximalsten Werten für die Vertraulichkeit, Integrität und Verfügbarkeit (Maximumprinzip). Deutlicher wird dies anhand eines Beispiels. Das Asset OSIS hat einen Schutzbedarf von 9, was den höchst möglichen Wert darstellt. Dieser errechnet sich daraus, dass sowohl die Vertraulichkeit, als auch die Integrität und Verfügbarkeit bei mindestens einer der Auswirkungskategorien auf sehr hoch (3) steht. Alle Werte werden addiert, sodass sich der Schutzbedarf von 9 ergibt.

Schutzbedarf der Zielobjekte						
Index	Bezeichnung	Anwendungsbeschreibung	Vertraulichkeit	Integrität	Verfügbarkeit	Schutzwert*
S_1	BHT/WHT	Bremer Hafentelematik	3	3	2	**8**
S_2	OSIS	Vernetzung unternehmensinterner Prozesse	3	3	3	**9**
S_3	ALPO	schnelle und sichere Kommunikation mit den Informationssystemen von nationalen und internationalen Seehäfen	3	3	2	**8**
S_4	ATLAS	Automatisiertes Tarif- und Lokales Zollabwicklungssystem	3	3	3	**9**

Abbildung Schutzbedarfsfeststellung Zielobjekte

Im nächsten Schritt werden alle relevanten lokale Risiken den einzelnen Assets zugeteilt. Im Anschluss wird die Eintrittswahrscheinlichkeit definiert. Diese wird mit dem Schutzbedarf des Assets multipliziert. Der Produktwert der Multiplikation ergibt das Brutto-Risiko. Risikowerte von 3-12 sind grundsätzlich als geringes Risiko einzustufen, sodass eine Risikoakzeptanz möglich ist. Risikowerte von 14-25 sind dem mittleren Risiko zuzuordnen. Eine Risikoakzeptanz ist nur durch die Freigabe des Abteilungsleiters möglich. Risikowerte von 27-45 sind dem hohen Risiko zuzuordnen. Hier gilt, dass eine Risikoakzeptanz nur durch die Freigabe der Geschäftsführung möglich ist.

Schutzbedarf (Auswirkung)	Eintrittswahrscheinlichkeit 1	2	3	4	5
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25
6	6	12	18	24	30
7	7	14	21	28	35
8	8	16	24	32	40
9	9	18	27	40	45

Abbildung Risikomatrix

Je nach Brutto-Risiko wird eine entsprechende Risikobehandlung festgelegt und anhand dessen das Netto-Risiko ermittelt. Des Weiteren wird das Risiko an ein mögliches ISO/IEC 27001 Control geknüpft.

	Asset	Schutzbedarf*	Lokale Gefährdung	Eintrittswahrscheinlichkeit (vor Risikobehandlung)	Risiko (Brutto)
A-1	BHT/WHT	8	R_1	1	8
			R_2	1	8
			R_8	3	24
			R_10	2	16
A-2	OSIS	9	R_17	4	36

Abbildung Brutto-Risiko

AP 1.5: In Arbeitspaket 1.5 hat die dsc zusammen mit den anderen Partnern mögliche Sicherheitsanforderungen bzw. Sicherheitsmaßnahmen aufgestellt, die den ermittelnden Risiken entgegenwirken können. Diese Sicherheitsanforderungen wurden mit in die Risikoanalyse integriert und direkt auf vorhandene Risiken angewendet, sodass jeweils ein mögliches Netto-Risiko ermittelt werden konnte. Z.B. wurde für das Risiko „Eine Manipulation der Zollfreigabe/Reederfreistellung führt dazu, dass Container fälschlicherweise verschickt bzw. zurückgehalten werden. Dies sorgt überdies für massive Störungen im Verladeprozess.“ des Assets BHT (Bruttorisiko = 24) die Maßnahme „Senkung der Eintrittswahrscheinlichkeit durch den Einsatz einer **2-Faktor-Authentisierung** in Kombination mit einer **Signierung.“** definiert. Dadurch wird die Eintrittswahrscheinlichkeit von 3 auf 1 gesenkt. Das Nettorisiko beläuft sich auf den Wert 8 (geringes Risiko). Dieses Vorgehen wurde für alle Assets und Risiken durchgeführt.

Risikobehandlung	Maßnahme	Eintrittswahrscheinlichkeit (nach Risikobehandlung)	Risiko (Netto)	Betroffenes Control der ISO/IEC 27001	Kommentar
Risikoakzeptanz	/	1	8	A.12, A.13	Brutto Risikowert unterschreitet Risikoakzeptanz
Risikoakzeptanz	/	1	8	A.12, A.13	Brutto Risikowert unterschreitet Risikoakzeptanz
Risikominderung	Senkung der Eintrittswahrscheinlichkeit durch den Einsatz einer **2-Faktor-Authentisierung** in Kombination mit einer **Signierung**	1	8	A.9.1.1, A.9.4.2, A.13.1	R_8 bringt ein großes Integritätsproblem mit sich, die z.B. durch den Einsatz von erweiterten Zugangskontrollmechanismen beseitigt werden können.

Abbildung Netto-Risiko

AP 1.6: In Unterarbeitspaket 1.6 wurde parallel zu den Untersuchungen in AP 1.1 bis AP 1.5 die Gesetzeslage im Hafenumfeld überprüft. Dabei wurden insbesondere spezielle Anforderungen der einzelnen Akteure, wie z.B. das IT-Sicherheitsgesetz, als auch allgemeingeltende Verordnungen und Gesetze wie die DSGVO, berücksichtigt. In Zusammenarbeit zwischen dem Justiziariat und der Informationssicherheit der dsc wurde zunächst definiert, was ein HKV und eine kritische Infrastruktur im generellen überhaupt ist und wie diese rechtlich einzuordnen sind. In dem 41-seitigen Gutachten wird im Detail beschrieben, welche Handlungshilfen es zur Umsetzung von KRITIS im HKV gibt. Dabei wird erläutert, was ein ISMS ist, was unter den Begrifflichkeiten Verfügbarkeit, Authentizität, Integrität und Verfügbarkeit zu verstehen ist und welche spezifischen Anforderungen eine kritische Infrastruktur sonst noch alle erfüllen müssen (z.B. Kontaktstelle beim BSI). Das gesamte Kapitel 2 widmet sich ausschließlich des Datenschutzes und der Datensicherheit. Dabei werden notwendige Aspekte der DSGVO aufgegriffen, erklärt und eine mögliche Handlungshilfe näher beschrieben. Z.B. verpflichtet die DSGVO gemäß Art. 5 Abs. 1 lit. die Verantwortlichen dazu, die Integrität und Vertraulichkeit der verarbeiteten personenbezogenen Daten zu gewährleisten. Dies muss unter anderem durch ausreichende technische und organisatorische Maßnahmen erfolgen. Als mögliche Handlungshilfe wird vorgegeben:

„Teilnehmer im HKV haben als Verantwortliche die IT-Sicherheit der Daten sicherzustellen und nachzuweisen. Kritische IT-Systeme, -Komponenten und -Prozesse sind also durch angemessene Vorkehrungen nach dem Stand der Technik gegen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit abzusichern. Hierbei ergeben sich zahlreiche Überschneidungen sowie Synergien zu einer KRITIS-konformen Aufstellung nach BSIG. Das setzt voraus, dass der Verbund entsprechende Sicherheitsmaßnahmen umsetzt und nachweist, etwa durch Audits und mittels sogenannter Penetrationstests, welche die relevanten IT-Systeme auf Schwachstellen prüfen. Dienstleister, wie die dbh Logistics IT AG

und die DAKOSY Datenkommunikationssystem AG, sowie alle Dienstleister, welche gemäß Art. 28 DSGVO Auftragsverarbeitungen vornehmen, sind schriftlich auf die Einhaltung dieser Sicherheitsmaßnahmen zu verpflichten (siehe unten zur Auftragsverarbeitung) und regelmäßig zu kontrollieren (dazu unten zur Rechenschaftspflicht)".

AP 6:

Die Digitalisierung ist heutzutage aus sämtlichen Branchen nicht mehr wegzudenken, so auch nicht auf dem Bereich Transport und Verkehr. Modernste IT-Systeme und Anlagen sorgen dafür, dass alle Prozesse in dieser Branche Hand in Hand einhergehen mit Informationstechnik und von dieser nahezu abhängig sind. Eine Logistikbranche ohne den Einsatz hochkomplexer IT-Systeme ist heutzutage nicht mehr denkbar, da diese nicht nur maßgeblich als Impulsgeber und Innovationsbeschleuniger sondern auch als Wegbereiter neuer Geschäftskonzepte gelten. Ein akutes Wegbrechen der IT-Systeme hätte je nach Größe des Unternehmens maßgebliche Auswirkungen für die deutsche Wirtschaft.

Um derartige Szenarien zu verhindern, hat der Gesetzgeber das IT-Sicherheitsgesetz ins Leben gerufen. Das IT-Sicherheitsgesetz verfolgt das Ziel der Verbesserung der IT-Sicherheit von Unternehmen in Deutschland. Der Fokus steht dabei auf den kritischen Infrastrukturen wie z.B. der Strom- und Wasserversorgung. Kritische Infrastrukturen werden grundsätzlich wie folgt definiert:

> *„Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden."*

Die Betreiber dieser kritischen Infrastrukturen, egal ob privatwirtschaftlich oder öffentlich organisiert, haben Sorge zu tragen, dass die Qualität und Stabilität ihrer Dienstleistungen zu jedem Zeitpunkt ausreichend gegeben sind.

Um dies zu gewährleisten müssen sich alle Betreiber, die gemäß der KRITIS-Verordnung (BSI-KritisV) als Betreiber einer kritischen Infrastruktur gelten, alle zwei Jahre einen Prüfnachweis gemäß §8a BSIG erbringen. Hierfür kann ein Branchenspezifischer Sicherheitsstandard (B3S) oder eine gleichwertige Prüfgrundlage (nicht offiziell vom BSI freigegeben) herangezogen werden. Kritische Infrastrukturen sind bei der Umsetzung der Anforderung (welche sich aus dem §8a BSIG als auch dem IT-Sicherheitskatalog ergeben) frei in der Wahl der Prüfgrundlage, insofern diese den gesetzlichen Anforderungen entsprechen.

Grundsätzlich wird in neun einzelnen Sektoren kritischer Infrastrukturen unterteilt, die wiederum in weitere Bereiche unterteilt werden. So gibt es die Sektoren Energie, Gesundheit, IKT, Transport und Verkehr, Medien und Kultur, Wasser, Finanz- und Versicherungswesen, Ernährung sowie Staat und Verwaltung. Bei SecProPort wurde alleinig der Sektor Transport und Verkehr betrachtet und beschränkt sich dabei auf die Unterbereiche, die sich auf der einen Seite mit Seefrachtlogistik und auf der anderen Seite mit der Leitzentrale von Betreibern und Verkehrsunternehmen der Seeschifffahrt beschäftigen.

Im Rahmen des sechsten Arbeitspaketes wurde daher ein individueller Prüfstandard entwickelt, mit relevanten Partnern abgestimmt und am Ende exemplarisch evaluiert. Zunächst wurde durch ein Brainstorming mit verschiedenen Mitarbeitern der datenschutz cert analysiert, aus welchen Bestandteilen sich der Prüfstandard zusammensetzen muss. Die Vorgaben zur Erstellung eines derartigen Standards werden vom Bundesamt für Sicherheit in der Informationstechnik bereitgestellt. Die dafür vorhandene „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a Absatz 2 BSIG" wurde dabei eingehalten, sodass der Standard den Ansprüchen eines vom BSI freigebenden Prüfstandards entspricht.

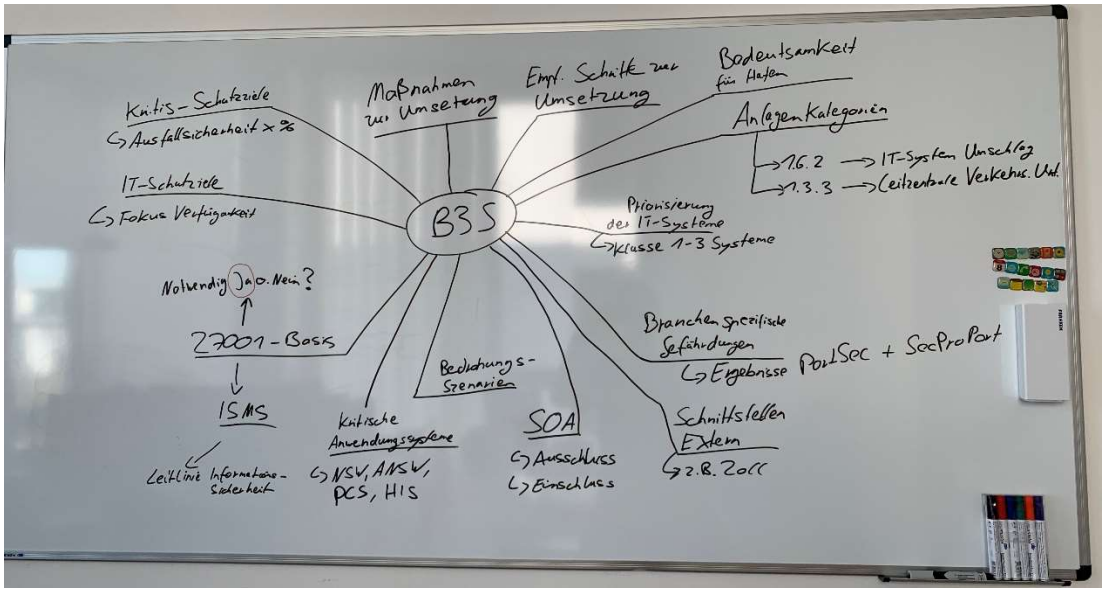


Abbildung Brainstorming B3S

Bereits zu Beginn der Planungsphase (kurz nach Projektbeginn) wurde festgelegt, dass die Prüfgrundlage auf Basis der ISO-Norm ISO/IEC 27001 aufgebaut werden soll, welche Anforderungen für die Erstellung und Aufrechterhaltung eines Informationsmanagement-Systems (ISMS) vorgibt. Die

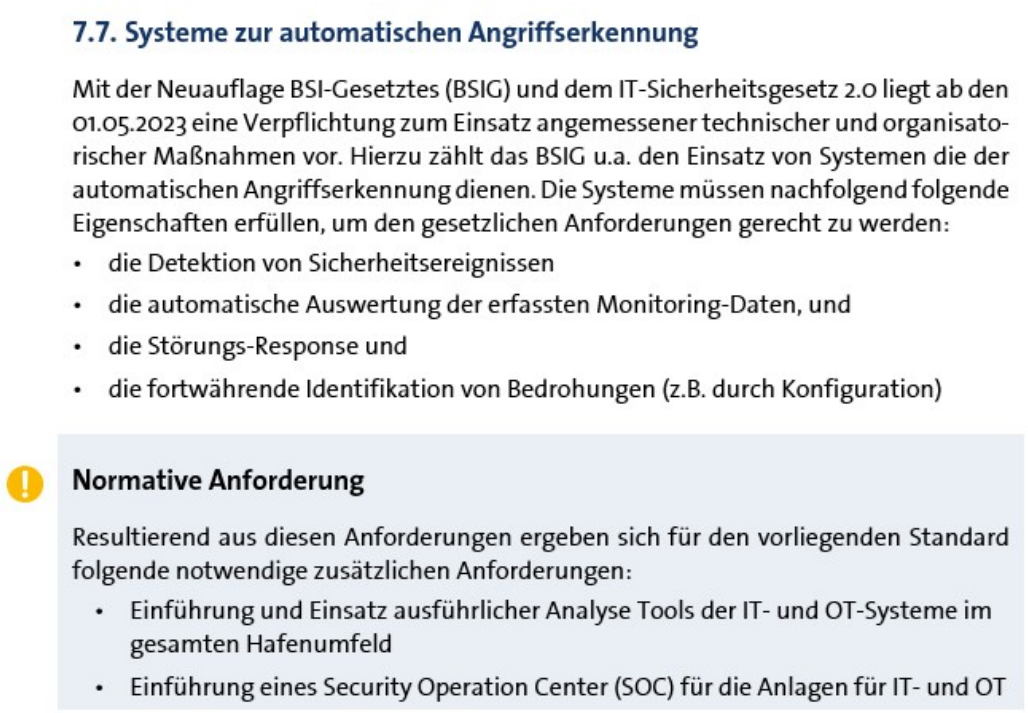
normativen Aspekte der ISO/IEC 27001 werden dabei als Basis-Anforderungen in der Prüfgrundlage angesehen, welche um wesentliche gesetzliche und branchenspezifische Anforderungen ergänzt wurden. Die gesetzlichen Anforderungen haben sich dabei in Laufe der Projektdauer kontinuierlich verändert. Folgende Gesetze wurden maßgeblich beachtet:

- BSIG (vor allem §8a)
- IT-Sicherheitsgesetz 1.0 und 2.0
- DSGVO
- BDSG-neu
- BBKG
- LDSG der Bundesländer
- Verordnung (EG) Nr. 725/2004 zur Gefahrenabwehr auf Schiffen und in Hafenanlagen
- Seeaufgabengesetz zur Abwehr von Gefahren für die Sicherheit und Leichtigkeit des Verkehrs, die Verhütung von der Seeschifffahrt ausgehender Gefahren und schädlicher Umwelteinwirkungen auf den Seewasserstraßen und Binnenwasserstraßen sowie in den an ihnen gelegenen bundeseigenen Häfen.
- Identitätsfeststellungen gem. § 23 des Gesetzes über die Bundespolizei (BPolG)
- Identitätsfeststellung gem. § 10 Zollverwaltungsgesetz (ZollVG)
- Hafensicherheitsgesetze der Bundesländer

Neben den gesetzlichen Anforderungen wurden auch branchenspezifische Anforderungen ergänzt, welche speziell auf die Seefrachtlogistik und Hafentelematik-Systeme abzielen. Dafür wurde in Arbeitspaket 1 eine Risikoanalyse-Methodik erstellt, anhand dessen in gemeinsamer Arbeit mit den anderen Projektpartnern in Laufe der Projektzeit lokale und globale Gefährdungen im gesamten Hafenumfeld hinsichtlich ihrer Kritikalität bewertet und mögliche Gegenmaßnahmen abgeleitet werden konnten. Diese Maßnahmen wurden anschließend in der Prüfgrundlage den jeweiligen Normkapiteln thematisch zugeordnet. Neben den Basis-Anforderungen der ISO/IEC 27001 (ca. 14 Sicherheitsthemen, 35 damit verbundenen Maßnahmenzielen und 114 Controls) konnten somit 41 weitere spezifische Maßnahmen ergänzt werden, welche z.T. noch mehrere Unter-Maßnahmen beinhalten. Hierzu gehören z.B. Maßnahmen wie:

- Systeme zur automatischen Angriffserkennung (siehe Abbildung unten)
- KRITS-Schutzziele

- Einführung eines Mobile-Device-Managements
- 24/7 Meldestelle
- 4-Augen-Prinzip bei der Berechtigungsvergabe
- Assetmanagement für OT-Komponenten
- PKI
- Zero-Trust-Architecture
- Ausführliche Physikalische Sicherheitsmaßnahmen (z.B. automatische Löschanlage von IT und Technikräumen)
- Regelmäßige Durchführung von Penetrationstests
- Einhaltung der Hafenspezifischen Gesetzeslage
- Usw.



7.7. Systeme zur automatischen Angriffserkennung

Mit der Neuauflage BSI-Gesetztes (BSIG) und dem IT-Sicherheitsgesetz 2.0 liegt ab den 01.05.2023 eine Verpflichtung zum Einsatz angemessener technischer und organisatorischer Maßnahmen vor. Hierzu zählt das BSIG u.a. den Einsatz von Systemen die der automatischen Angriffserkennung dienen. Die Systeme müssen nachfolgend folgende Eigenschaften erfüllen, um den gesetzlichen Anforderungen gerecht zu werden:

- die Detektion von Sicherheitsereignissen
- die automatische Auswertung der erfassten Monitoring-Daten, und
- die Störungs-Response und
- die fortwährende Identifikation von Bedrohungen (z.B. durch Konfiguration)

Normative Anforderung

Resultierend aus diesen Anforderungen ergeben sich für den vorliegenden Standard folgende notwendige zusätzlichen Anforderungen:

- Einführung und Einsatz ausführlicher Analyse Tools der IT- und OT-Systeme im gesamten Hafenumfeld
- Einführung eines Security Operation Center (SOC) für die Anlagen für IT- und OT

Abbildung Beispiel - automatische Angriffserkennung

Nachdem der Prüfstandard finalisiert werden konnte und alle zu dem Zeitpunkt eingetretenen Individualitäten berücksichtigt werden konnten (Anpassung BSIG und der KRITIS-Verordnung), wurde dieser in einem Arbeitsmeeting mit den Partnern noch einmal final vorgestellt und abgestimmt. Nach Einbringung von Feedback wurde der Prüfstandard dann in der Praxis evaluiert und die dbh anhand

dessen auditiert. Die Auditierung hat gezeigt, dass der Prüfstandard sehr gut für eine Auditierung von Unternehmen ist, welche bereits ein ISMS nach ISO/IEC 27001 haben. Der Vorteil des generischen Standards ist, dass sich dieser auf verschiedene Akteure im Hafenumfeld anwenden lässt, egal ob IT-Dienstleister, Spediteur oder Terminalbetreiber.

Von einer Einreichung des Prüfstandards beim BSI wurde abgesehen, da einer der führenden Verbände im Bereich der Hafenlogistik sich dessen kritisch geäußert hat. Trotzdem kann, darf und wird der Standard weiterhin angewendet, da Unternehmen frei in der Wahl der Prüfgrundlage sind und nicht auf abgenommene Branchenspezifische Sicherheitsstandards zurückgreifen müssen.

2.2 Wichtigste Positionen des zahlenmäßigen Nachweises

Die im Vorfeld geplanten Kosten des Projektes konnten nahezu vollständig, trotz der Corona-Pandemie, verrechnet werden. Auf Grund der Corona-Pandemie konnten ab 2020 jedoch nahezu keine Reisekosten verrechnet werden. Starke Abweichungen gibt es in Summe nicht.

2.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Der Bereich der Informationssicherheit ist für viele Unternehmen noch recht neu und es gibt nur wenig spezialisiertes Fachpersonal in diesem Bereich. Trotzdem ist die Informationssicherheit aus Unternehmen und Konzernen, vor allem kritischen Infrastrukturen gar nicht mehr wegzudenken. Die datenschutz cert GmbH ist bereits seit vielen Jahren als akkreditierte Zertifizierungsstelle (DAkkS und BSI) tätig und kann viele Erfahrungen in diesem Umfeld vermitteln. Die Teilhabe an SecProPort war notwendig, da eine Erstellung eines Prüfstandards für Praxispartner ohne direkten Informationssicherheitsbezug nur schwer möglich ist. Gleiches gilt für die Analyse der rechtlichen Infrastruktur im Hafen sowie der Erstellung einer Risikoanalyse-Matrix, welche für den Demonstrator von essentieller Bedeutung war.

2.4 Voraussichtlicher Nutzen und Verwertbarkeit des Ergebnisses

Die datenschutz cert GmbH wird die Ergebnisse auf verschiedenen Ebenen weiterverwenden. So dient die Risikoanalysematrix vor allem den Beratern aus der Schwesterfirma der dsn Security, welche kritische Infrastrukturen beraten und u.a. dabei unterstützen ein §8a BSIG konformes ISMS aufzubauen. Die entwickelte Risikoanalyse wird den Kunden dabei als mögliches Vorgehen bzw. Best

Practice vorgestellt und bereits aktiv verwendet. Die datenschutz cert GmbH, welche auf Grund der Akkreditierung bei der DAkkS darf selber nicht beratend tätig sein, sondern lagert Beratungsvorhaben unmittelbar um auf die dsn Security. Gleiches gilt für die erstellte Prüfgrundlage. Unternehmen, welche ganz am Anfang stehen wissen i.d.R. noch nicht, worauf diese im KRITIS-Umfeld achten müssen. Konkrete Handlungshilfen, wie die erstellte Prüfgrundlage, können dadurch bereits im Beratungsumfeld eingesetzt werden und die Unternehmen im späteren Verlauf auf dessen Basis auditiert werden. Die Prüfgrundlage wird ferner stetig gemäß veröffentlichten Gesetzen aktualisiert. Grundsätzlich konnten während der Projektlaufzeit immer mehr kritische Infrastrukturen, auch aus dem Bereich der Hafentelematik, durch uns auditiert und zertifiziert werden. Dies zeigt, dass der Markt und das Interesse, wenn auch getrieben durch gesetzliche Anforderungen, an einer derartigen Zertifizierung groß ist.

Auch Penetrationstests werden immer häufiger angefragt und durch die datenschutz cert bzw. durch den zertifizierten Penetrationstester Michael Cyl durchgeführt. Zwar stammen auch hier einige Neukunden aus dem KRITIS-Umfeld, jedoch weniger aus dem Bereich der Hafentelematik. Wie bereits oben beschrieben, führt bremenports das Thema der Penetrationstests im Hafenumfeld weiter fort. Da dieser immer noch auf geringfügiger Basis bei der datenschutz cert GmbH angestellt ist, ist dieser weiterhin berechtigt, Penetrationstests im Rahmen der datenschutz cert GmbH durchzuführen.

ZEITSCHIENE

2.5 Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen

/

2.6 Erfolgte und geplante Veröffentlichungen

Neben den Prüfstandard, welche kostenlos an Interessenten herausgegeben wird, sind keine weiteren Veröffentlichungen geplant.

3 Literatur

/

4 Anhang

Berichtsblatt

1. ISBN oder ISSN	**2. Berichtsart (Schlussbericht oder Veröffentlichung)** Schlussbericht
3. Titel Abschlussbericht - Verbundprojekt SecProPort	
4. Autor(en) [Name(n), Vorname(n)] Aiko Czembor, Sönke Maseberg	**5. Abschlussdatum des Vorhabens** 31.12.2021
	6. Veröffentlichungsdatum 07.03.2022
	7. Form der Publikation Schlussbericht
8. Durchführende Institution(en) (Name, Adresse) datenschutz cert GmbH	**9. Ber.-Nr. Durchführende Institution**
	10. Förderkennzeichen 19H18012D
	11. Seitenzahl 20
12. Fördernde Institution (Name, Adresse) Bundesministerium für Digitales und Verkehr Invalidenstraße 44 D-10115 Berlin	**13. Literaturangaben**
	14. Tabellen
	15. Abbildungen
16. DOI (Digital Object Identifier)	
17. Vorgelegt bei (Titel, Ort, Datum) Abschlusschlussbericht - SecProPort; Bremen; 07.03.2022	
18. Kurzfassung Ziel des Vorhabens SecProPort war es, eine Sicherheitsarchitektur für den Hafenkommunikationsverbund systematisch auf Basis einer Prozess- und Bedrohungsanalyse zu entwickeln. Diese Sicherheitsarchitektur erfüllt Resilienzanforderungen , so dass das Gesamtsystem auch im Falle eines Angriffs weiterarbeitet. Aus der Sicherheitsarchitektur wurden anschließend Sicherheitsanforderungen für die Anwendungen der einzelnen Hafenakteure abgeleitet und Migrationspläne entwickelt. Bei einzelnen Anwendungspartnern wurde die Sicherheitsarchitektur beispielhaft umgesetzt, um ihre praktische Relevanz nachzuweisen. Die Projektergebnisse sind zudem in einen branchenspezifischen Standard für die Informationssicherheit im Bereich Hafen eingeflossen.	
19. Schlagwörter Hafentelematik, IT-Sicherheit, Informationssicherheit, Branchenspezifischer Sicherheitsstandard, Zertifizierung, Penetrationstest	
20. Verlag	**21. Preis**

Entwurf

Document control sheet

1. ISBN or ISSN	**2. type of document (e.g. report, publication)** Veröffentlichung (Publikation)
3. title Joint project: SecProPort - Scalable security architectures for business processes in German ports;	
4. author(s) (family name, first name(s)) Aiko Czembor, Sönke Maseberg	**5. end of project** 31.12.2021
	6. publication date 07.03.2022
	7. form of publication Document Control Sheet
8. performing organization(s) name, address datenschutz cert GmbH	**9. orginators report no.**
	10. reference no. 19H18012D
	11. no. of pages 20
12. sponsering agency (name, address) Bundesministerium für Digitales und Verkehr Invalidenstraße 44 D-10115 Berlin	**13. no. of references**
	14. no. of tables
	15. no. of figures
16. DOI (Digital Object Identifier)	
17. presented at (title, place, date) Abschlussbericht Verbundprojekt SecProPort; bremen; 07.03.2022	
18. abstract The aim of the SecProPort project was to systematically develop a security architecture for the port communications network on the basis of a process and threat analysis. based on a process and threat analysis. This security architecture meets resilience requirements so that the overall system continues to operate even in the event of an attack. The security architecture was then used to derive security requirements for the applications of the individual port stakeholders and to develop migration plans. At individual application partners, the security architecture was implemented as an example to demonstrate its practical relevance. The project results have also been incorporated into an industry-specific standard for information security in the port sector.	
19. keywords Port telematics, IT security, information security, industry-specific security standard, certification, penetration test	
20. publisher	**21. price**

Nicht änderbare Endfassung mit der Kennung 1630344-2