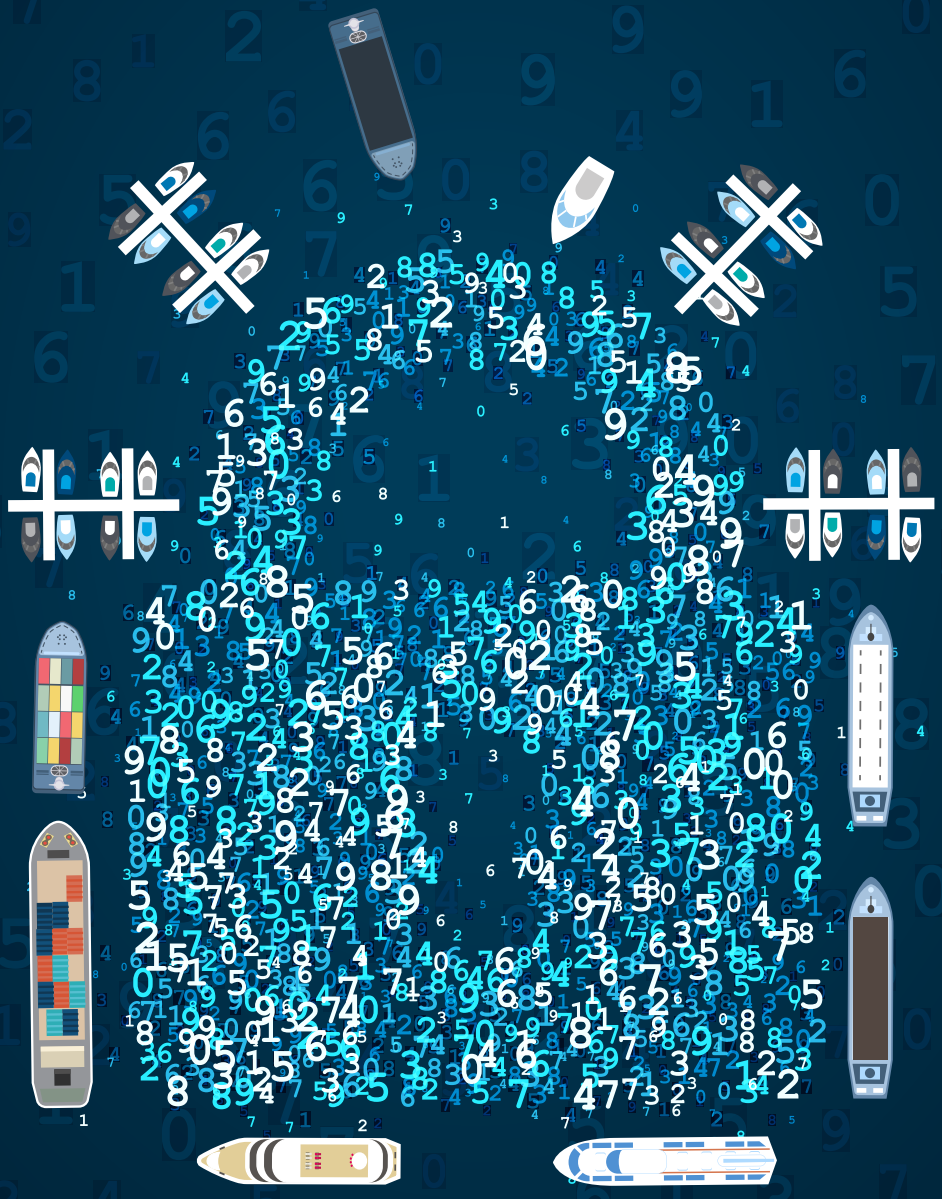
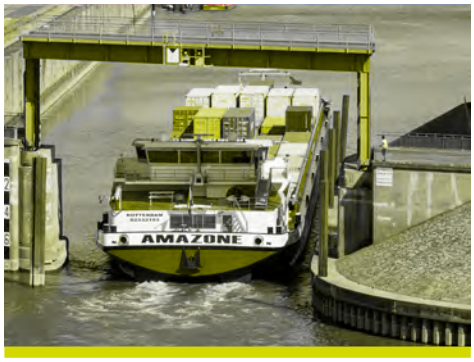
Good-Practice-Leitfaden Cybersicherheit in der Binnenschifffahrt

Schwerpunkt Häfen



Inhaltsverzeichnis



Einleitung

Hintergrund

Ein Leitfaden auf Anregung des Europäischen Ausschusses für die Ausarbeitung von Standards im Bereich der Binnenschifffahrt (CESNI)

Die Aufgaben des Europäischen Ausschusses für die Ausarbeitung von Standards im Bereich der Binnenschifffahrt bestehen insbesondere darin :

- in verschiedenen Bereichen, namentlich den Bereichen Binnenschiffe, Informationstechnologie und Besatzung, technische Standards zu erlassen, auf welche die entsprechenden Regelwerke auf europäischer und internationaler Ebene, darunter die der Europäischen Union (im Folgenden „EU“) und der Zentralkommission für die Rheinschifffahrt, mit dem Ziel ihrer Anwendung verweisen können;
- über wichtige Themen der Sicherheit der Schifffahrt, des Umweltschutzes und anderer Bereiche der Binnenschifffahrt zu beraten.

Die von den Verkehrsministern der Mitgliedstaaten der Zentralkommission für die Rheinschifffahrt (ZKR) verabschiedete Mannheimer Erklärung[1] und das Aktionsprogramms NAIADES[2] der Europäischen Kommission bezeichnen beide die Digitalisierung als ein für die Zukunft der Binnenschifffahrt strategisches Thema. Diese Digitalisierung bringt neue Risiken und Herausforderungen wie die der Cybersicherheit mit sich.

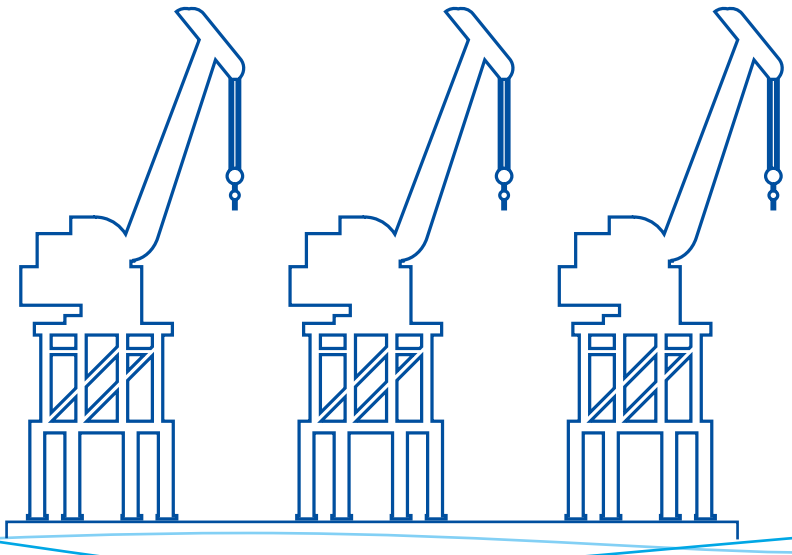
In Partnerschaft mit dem Europäischen Verband der Binnenhäfen (EFIP) beschloss der CESNI daher, für die Binnenhäfen einen Leitfaden zu bewährten Verfahrensweisen für die Cybersicherheit auszuarbeiten.

Relevanz für die Binnenhäfen

Durch die zunehmende Vernetzung der Welt und die wachsende Abhängigkeit von digitalen Dienstleistungen kommt es zu ständig neuen Cyberangriffen. Mehrere Häfen waren in den letzten Jahren bereits Zielscheiben von Cyberangriffen, womit deutlich wird, dass dieser Sektor keine Ausnahme darstellt.

So wurde zum Beispiel im Juni 2017 der Terminal des Unternehmens APM an der Maasvlakte des Rotterdamer Hafens von einem Schadprogramm (Ransomware) befallen. Der Rotterdamer Hafen erlitt erhebliche Beeinträchtigungen durch das Virus und verzeichnete eine in Tagen messbaren Betriebsunterbrechung. Kräne fielen aus und die Containerabfertigung stand still. Die Auswirkungen dieses Cyberangriffs waren im gesamten Ökosystem des Hafens und Seeverkehrs spürbar und bestätigten einmal mehr die bekannte Tatsache, dass sich Cyberbedrohungen schon längst nicht mehr auf rein IT-abhängige Sektoren beschränken.

Mit ihrer fortschreitenden Vernetzung, Digitalisierung und Abhängigkeit von modernen IT-Systemen werden Häfen wie Rotterdam anfälliger für derartige Cyberangriffe[3].



[1] https://www.ccr-zkr.org/files/documents/dmannheim/Mannheimer_Erklaerung_de.pdf
[2] https://transport.ec.europa.eu/transport-modes/inland-waterways/promotion-inland-waterway-transport/naiades-iii-action-plan_en
[3] https://www.dutchnews.nl/news/2017/06/smart-port-in-rotterdam-confounded-by-cyber-attack/

Wer auf solche Bedrohungen reagieren will, sollte ein klares Verständnis davon besitzen, was Cyberrisiken im Umfeld von Binnenhäfen bedeuten und wie man sie mindern kann. Einige Binnenhäfen arbeiten im Alltagsbetrieb noch nicht mit verbundenen physischen Assets. Deshalb haben sie vielleicht nicht den Eindruck, dass sie von der Frage der Cybersicherheit betroffen sind, aber es lässt sich nicht leugnen, dass diese Häfen nach und nach zunehmend vernetzt sein werden. Sie werden immer mehr in die Sicherung von Assets wie komplexe Logistiksoftware, vernetzte Kamera- und Gating-Systeme, Fernnavigationsprogramme, Anwendungen für das Containermanagement und andere „smarte" Technologien zur Effizienzsteigerung des Hafenbetriebs investieren müssen, die anfällig für Cyberangriffe sind. Die Verbesserung der Cybersicherheit ist also nicht nur eine Frage der verstärkten Sicherheit von Computer- und IT-Systemen in Binnenhäfen. Sie setzt auch die Förderung eines verstärkten Bewusstseins für Cybersicherheit bei den Hafenbeteiligten voraus, die mit verschiedenen Arten von verbundenen Geräten arbeiten, um diverse hafenbezogene Dienstleistungen anzubieten.

Vor diesem erweiterten Hintergrund möchte der vorliegende Leitfaden einen leicht verständlichen Rahmen für die Darstellung bewährter Verfahrensweisen für den Betrieb von Binnenhäfen bieten[4].

Anwendungsbereich dieses Leitfadens und Hinweise für seine Lektüre

Generell gibt es fünf Möglichkeiten, auf ein Cybersicherheitsrisiko einzugehen:

1. das Risiko akzeptieren, d. h. nichts zu tun und die Konsequenzen auf sich nehmen;
2. das Risiko vermeiden, d. h. es durch radikale Maßnahmen vollständig ausschalten, in dem man beispielsweise eine Schleuse aus dem Betrieb nimmt, den Hafen für die Schifffahrt sperrt oder ihn für bestimmte Schiffe verbietet, die ein gewisses Risiko darstellen könnten;
3. das Risiko übertragen, indem man z. B. eine Versicherung abschließt oder einen Dritten beauftragt, der die Folgen anstelle des Hafens trägt;
4. das Risiko teilen, d. h. eine Vereinbarung mit Dritten treffen, um die Kosten oder die Folgen gemeinsam zu tragen, wenn der Risikofall eintritt;
5. das Risiko mindern, d. h. verschiedene Maßnahmen ergreifen, mit deren Hilfe die Eintretenswahrscheinlichkeit des Risikos verringert oder dessen Folgen begrenzt werden.

Dieser Leitfaden verfolgt in erster Linie den Ansatz der **Risikominderung**. Er umfasst einige Elemente, die in die Kategorien Übertragung oder Teilen des Risikos fallen. Es soll darauf hingewiesen werden, dass jedes Nichttätigwerden im Hinblick auf die Cybersicherheit de facto bedeutet, alle Risiken auf sich zu nehmen, seien sie bekannter oder unbekannter Natur.

Dieser Leitfaden soll einen Überblick über Cyberrisiken, -bedrohungen und -abwehrmaßnahmen bieten, der sich in erster Linie auf das Gebiet der Binnenhäfen konzentriert. Er möchte dem Zielpublikum (siehe unten) ein besseres Bild der Verursacher von Cyberangriffen und ihrer Handlungsmotive sowie der Anlagewerte der Binnenhäfen vermitteln, die bei der Einschätzung der Bedrohungen und Risiken im Cyberbereich zu berücksichtigen sind. Dieser Leitfaden bietet außerdem einen Überblick über bewährte Verfahrensweisen für die Umsetzung von Maßnahmen zur Minderung von Cyberrisiken.

[4] https://www.dutchnews.nl/news/2017/06/smart-port-in-rotterdam-confounded-by-cyber-attack/

Um eine bessere Vorstellung des Ökosystems Hafen zu vermitteln, werden in diesem Leitfaden auch schützenswerte Güter (im Folgenden: „Assets“) mit Bedeutung für Binnenschiffe aufgenommen.

Das Dokument ist in drei Teile unterteilt:

1. die Cyberbedrohungslandschaft in den Binnenhäfen: Beschreibung der Bedrohungslage in den Binnenhäfen mit ihren Akteuren, der Hafen-Assets, der Bedrohungstaxonomie und der Angriffsszenarien;
2. minderung von Cybersicherheitsrisiken für Binnenhäfen: Eine detaillierte Beschreibung des Portfolios von Maßnahmen zur Risikominderung, die zur Verbesserung der Cybersicherheit in Häfen ergriffen werden können;
3. tipps zur Umsetzung der Risikominderungsmaßnahmen: Skizzierung umsetzbarer Maßnahmen für eine Sicherheitshygiene als erste Schritte für IT- und Nicht-IT-Beteiligte.

Der vorliegende Leitfaden ist als Orientierungshilfe für Hafenbeteiligte gedacht und soll keinen Ersatz für bereits veröffentlichte Methoden zur Risikobewertung im Bereich Cybersicherheit darstellen. Er soll hingegen allen beteiligten Parteien ermöglichen, die für die Bewertung und den Umgang mit Cyberrisiken am besten geeigneten Maßnahmen zu ermitteln.

Zielpublikum des Leitfadens

Dieser Leitfaden richtet sich in erster Linie an die Hafenakteure, nämlich:

- die Hafenbehörden bzw. ihre Unterauftragnehmer;
- die Terminalbetreiber bzw. ihre Unterauftragnehmer;
- die Logistikunternehmen, die mit Hafenbehörden und Terminalbetreibern zusammenarbeiten.

Allerdings könnte dieser Leitfaden auch ein breiteres, indirekt von diesen Fragen betroffenes Publikum interessieren:

- die nationalen Binnenwasserstraßenbehörden;
- die Schifffahrtsunternehmen;
- die öffentlichen Einrichtungen mit Regelungsbefugnissen für die Binnenschifffahrt ;
- die Schiffsbetreiber;
- die Schiffsführer;
- die Schiffsbesatzungen;
- die Hersteller von Erzeugnissen für den Binnenschifffahrtssektor.

Innerhalb dieser Zielgruppe unterscheidet der Leitfaden zwischen drei Arten von Beteiligten, die eng in die Umsetzung der im Leitfaden vorgestellten bewährten Verfahrensweisen eingebunden werden müssen:

IT-Teams **Betriebsverantwortlichen** **Direktion**

Verweise auf internationale Normen und Standards

Dieser Leitfaden ist kein Ersatz für internationale Normen und Standards im Bereich der Cybersicherheit, oder gar für die bestehende Literatur zu diesem Thema. Sein Ziel besteht darin, die Themen der Cybersicherheit im einem für Binnenhäfen spezifischen Kontext einem breiten Publikum zugänglich zu machen.

Um den Inhalt konkreter zu machen, wird eine Reihe von Maßnahmen in Form von Empfehlungen und Praxisbeispielen vorgeschlagen, die auf dem Markt angewendet werden und den Grundsätzen der Norm ISO/IEC 27001 entsprechen.

Die Umsetzung dieses Leitfadens stellt an sich keinen Ansatz für die Anpassung an Standards dar, die zu einer Zertifizierung führen könnte. Der Leitfaden ermöglicht jedoch eine Annäherung an das Thema und eine Sensibilisierung für Cybersicherheitsfragen, die einen nachfolgenden formelleren Zertifizierungsprozess im Bereich der Cybersicherheit (z. B. ISO/IEC 27001) erheblich erleichtern können.

Die Einrichtung eines Managementsystems für Informationssicherheit (ISMS - Information Security Management System) stellt beispielsweise einen wichtigen Punkt bei der Umsetzung der Norm ISO/IEC 27001 dar. Diese Norm enthält die Anforderungen für die Einrichtung, Dokumentation, Umsetzung, Überwachung, Aufrechterhaltung und fortlaufende Verbesserung eines ISMS. Der Leitfaden geht auf diese Punkte weniger detailliert ein, beschreibt jedoch Maßnahmen zur Vorbereitung und Erleichterung der Einrichtung eines solchen ISMS, sollte eine Organisation sich zu dessen Einführung entschließen.

Verweise auf nationale Vorschriften

Genauso wenig wie dieser Leitfaden die internationalen Normen und Standards im Bereich der Cybersicherheit ersetzt, ersetzt er auch nicht die geltenden Vorschriften insbesondere auf nationaler Ebene, deren Anwendung gegebenenfalls Vorrang gegenüber diesem Leitfaden zukommt.

Im Rahmen der Verstärkung der Informationssicherheit der Häfen können (oder müssen) die örtlich bestehenden Vorschriften oder Empfehlungen von nationalen Agenturen oder internationalen Behörden Anwendung erfahren.

Zur Verwendung dieses Leitfadens

Wenn Sie diesen Leitfaden lesen, um sich ein **allgemeines Bild von der Cybersicherheits-Bedrohungsumgebung von Binnenhäfen** zu machen, beginnen Sie am besten mit Teil 1 dieses Leitfadens.

Teil 2 umfasst alle einem Hafen zur Verfügung stehenden Maßnahmen zur Minderung von Cyberrisiken. Hierbei handelt es sich um das Herzstück des Leitfadens mit ca. 120 Maßnahmen, die auf das Binnenhafenumfeld zugeschnitten sind und in drei Kategorien unterteilt wurden:

1. maßnahmen zu organisatorischen Strategien und Verfahren (OPP);
2. maßnahmen zu informationstechnologischen / betriebstechnischen Strategien (ITOT) sowie;
3. technische Sicherheitsmaßnahmen innerhalb der Cybersicherheit (TSM).

Diese Maßnahmen werden erläutert und entsprechend **dem angestrebten Reifegrad** für jeden Hafen in Stufen dargestellt.

Lesen Sie diesen Leitfaden im Hinblick auf **eine Umsetzung spezifischer Sicherheitsmaßnahmen oder um sich ein Bild von der Cybermaturität Ihrer Organisation** zu machen, beginnen Sie mit Teil 3. Dieser wurde verfasst, um die Implementierung der risikomindernden Maßnahmen aus Teil 2 zu erleichtern. Teil 3 kann unabhängig von den ersten beiden Teilen gelesen und als Checkliste genutzt werden, um zu überprüfen, ob Ihre Organisation die Maßnahmen umgesetzt hat, die ihren Zielsetzungen im Hinblick auf die Cybersicherheit entsprechen. Diese Tipps sollen für alle Zielgruppen eine leicht verständliche und informative Hilfe darstellen.

Teil 3 bietet eine „Anwendbarkeitstabelle", also ein Raster für die Einordung der risikomindernden Maßnahmen aus Teil 2, basierend auf den Zielen, die der Hafen im Bereich der Cybersicherheit anstrebt, dem Hafentyp und der Art von Beteiligten (IT-Teams, Betriebsverantwortliche und Geschäftsleitung).

Wenn Sie diesen Leitfaden als Einführung in die Cybersicherheit in Binnenhäfen nutzen, um sich einen Gesamtüberblick zu verschaffen, lesen Sie am besten den ganzen Leitfaden.

Izmail, Ukraine - Donau

Einige terminologische Elemente, die in diesem Leitfaden verwendet werden

Zur Erleichterung der Lektüre dieses Leitfadens wurden einige terminologische Begriffe vereinfacht.

Häfen

Wenn nicht ausdrücklich anders erwähnt, ist unter „Hafen“ ein Binnenschifffahrtshafen zu verstehen. Die Bezeichnung kann auch für einen gemischten Hafen stehen, d. h. für einen Hafen, in dem sowohl Binnen- als auch Seeschiffe verkehren, es sei denn, der Kontext erfordere eine Unterscheidung zwischen einem reinen Binnenschifffahrtshafen und einem gemischten Hafen.

Asset (Vermögenswert)

In diesem Leitfaden wird die Bezeichnung „Asset“ stets für „digitale Anlagewerte“ verwendet. Ein digitales Asset ist als Satz digitaler Daten definiert, dessen Eigentum oder Nutzungsrecht einen Teil des Vermögens eines Binnenschifffahrtshafens darstellt. (Digitale) Assets sind somit immaterielle Vermögenswerte. Dabei kann es sich beispielsweise um Daten oder Software handeln (Der Begriff „Daten“ ist hier sehr weit gefasst zu verstehen). Es wird darauf hingewiesen, dass ein digitales Asset bisweilen eng an einen klassischen, materiellen Vermögenswert gebunden sein kann, dessen ordnungsgemäßen Betrieb es sicherstellt. Eine Schleuse ist z. B. ein materielles Asset, für ihren Betrieb werden jedoch Software und viele spezifische Daten eingesetzt. Nicht alle materiellen Bestandteile der Schleuse, ihre Wände, Tore, aber auch Sensoren, Rechner, Datenkabel, Kameras usw. sind „Assets“ im Sinne dieses Leitfadens. Hingegen stellt die gesamte von einem beliebigen materiellen Bestandteil verwendete Software (mit ihren entsprechenden Einstellungen) einen digitalen Vermögenswert dar und gilt damit als „Asset“ im Sinne dieses Leitfadens.

IT/OT-Systeme

In einigen Abschnitten dieses Handbuchs wird auf IT/OT-Systeme Bezug genommen. In diesem Zusammenhang bezieht sich der Begriff IT (Information Technologies) auf den Teil des Systems, in dem die Informationsverarbeitung stattfindet. Dieser Teil ist weitreichend programmierbar und modifizierbar. Der Begriff OT (Operational Technologies) bezeichnet den Teil des Systems, der sich mit der Steuerung von Maschinen und physischen Abläufen befasst. Er ist in den meisten Fällen sehr autonom und für die Erfüllung bestimmter Aufgaben programmiert (beispielsweise für die Temperatur- oder Belüftungsregulierung). Vereinfacht gesagt werden über IT Daten verarbeitet, während über OT physische Objekte manipuliert werden. Diese beiden Systemtypen können natürlich miteinander interagieren, und das gilt in besonderem Maße für Fälle, in denen von „IT/OT-Systemen“ die Rede ist.

Cybersicherheit: Der Begriff wird in diesem Leitfaden sehr häufig verwendet, beginnend mit dem Titel. Im Rahmen dieses Leitfadens ist der Begriff „Cybersicherheit“ sehr weit gefasst zu verstehen. Es geht hier um die Anwendung einer Reihe von Techniken, Praktiken, Mitteln und Instrumenten zum Schutz von Informationssystemen und deren Daten. Auch dieser Schutz ist in einem weit gefassten Sinn zu verstehen: von der Prävention über die Erkennung und Reaktion auf Vorfälle bis zur Behebung von Schäden. Dabei kann es sich um informationstechnologische Angriffe, aber auch um Fahrlässigkeit, Unfälle, Naturkatastrophen oder menschliches Versagen handeln. Der Begriff „Cybersicherheit“ berücksichtigt nicht nur Bedrohungen informationstechnologischer Art, sondern auch solche, die sich aus physischen oder organisatorischen Aspekten ergeben. Daneben existieren auch andere Begriffe mit je nach Land und Kultur unterschiedlichen Bedeutungen, wie „Datensicherheit“ oder „Sicherheit von Informationssystemen“ oder auch „Informationssicherheit“.

Teil 1

Die Cyberbedrohungslandschaft in den Binnenhäfen

Allgemeine Tendenzen im Bereich der Cybersicherheit und ihre Auswirkungen auf die Binnenschifffahrt

Im Jahr 2020 veröffentlichte die Agentur der Europäischen Union für Cybersicherheit ENISA einen Bericht über die Bedrohungslandschaft für Seehäfen. Er gelangt zu den folgenden, im Kontext des Hafensektors besonders erwähnenswerten Erkenntnissen:

BEOBACHTETE TENDENZ	AUSWIRKUNGEN AUF BINNENHÄFEN
Bei den meisten Cyberangriffen ist nach wie vor das Streben nach finanziellem Gewinn das Hauptmotiv.	Als Knotenpunkte für Wirtschaftstransaktionen und Handel mit potenziell wertvollen Gütern können Binnenhäfen zur Zielscheibe von Personen werden, die aus finanziellem Interesse kriminelle Handlungen begehen wollen.
Gezielte und hartnäckige Angriffe auf hochwertige Daten wie geistiges Eigentum und Staatsgeheimnisse werden sorgfältig geplant und durchgeführt, vielfach von Akteuren mit staatlicher Unterstützung.	Als kritische Umschlagzentren, in denen wichtige Güter angeliefert werden, können Binnenhäfen zur Zielscheibe von Angriffen werden, wenn es um Informationen über die von ihnen aus belieferten Staaten geht.
Ransomware bleibt weit verbreitet, was kostspielige Konsequenzen für für zahlreiche Organisationen weltweit nach sich zieht.	Angriffe mit Ransomware stellen eine echte Bedrohung für die Welt der Binnenhäfen dar, deren Betrieb oft von der Verfügbarkeit der Systeme abhängt.
Die Anzahl potenzieller Sicherheitslücken in einer virtuellen oder physischen Umgebung erhöht sich durch den Eintritt in eine neue Phase des digitalen Wandels (in der sich die Technologie immer weiter diversifiziert).	Häfen zählen zu den Industriebereichen, in denen Projekte der digitalen Transformation besonders tiefgreifende Wirkung haben, insbesondere im Zusammenhang mit IT/OT-Konvergenz. Während dieser Umstellungen sollten Cybersicherheitsrisiken angemessen bewertet und gemindert werden.

Diese Erkenntnisse gelten für den Hafenkontext und weisen darauf hin, dass mangelnde Cybersicherheit als echter Risikofaktor bei den von den Häfen angebotenen kritischen Transport- und Wirtschaftsleistungen angesehen werden muss. Dementsprechend ist es ratsam, Maßnahmen zur Minderung dieses Risikos zu ergreifen.

Die IT-Sicherheit der Binnenhäfen, ihrer wichtigsten Assets sowie der Binnenschiffe

Vor jeder Prüfung der Bedrohungslage und der Ermittlung von Möglichkeiten für eine entsprechende Gefahrenabwehr muss die entsprechende Organisation zunächst verstehen, was genau geschützt werden soll. Zu diesem Zweck ist es sinnvoll, eine Kartierung der vorhandenen Assets vorzunehmen, bei der alle Assets, die sich als Zielscheibe für einen Cyberangriff bieten oder für einen solchen genutzt werden könnten, kartographisch dargestellt werden.

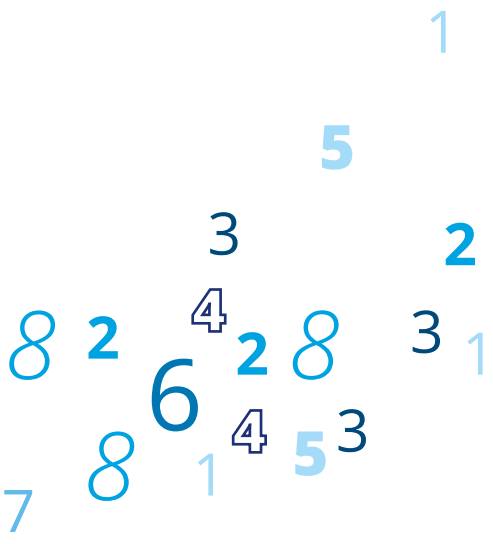
Zur Erleichterung dieser Aufgabe bietet dieser Leitfaden einen Rahmen für die Bewertung von Assets in Häfen und auf Schiffen. Auch wenn diese Assets nicht überall vorhanden oder für alle Zielgruppen von Bedeutung sind, soll die untenstehende Liste als Richtwert für die Bewertung der Assets in ihrem Umfeld verstanden werden. Es sei außerdem darauf hingewiesen, dass die Kritizität von Assets nicht für alle Organisationen die gleiche ist. So können in einem auf Warentransporte spezialisierten Hafen die Systeme zur Unterstützung des Betriebs eines Container-Terminals ein besonders kritisches Asset darstellen, während ein anderer Hafen dem zentralen Schleusenmanagementsystem besondere Bedeutung zuweist. Bei Häfen, die Dienstleistungen für die Fahrgastschifffahrt bieten, können die damit verbundenen Aktivitäten als kritische Tätigkeiten betrachtet werden. So besteht für eine Organisation der erste Schritt zu einem besseren Verständnis der bestehenden Sicherheitsrisiken und möglicher Minderungsmaßnahmen darin, eine vollständige Durchsicht aller Assets vorzunehmen. Ziel dabei ist, die für ihr Umfeld kritischen Assets zu identifizieren und eine Liste von **„Kronjuwelen“** (Vermögenswerte, die die die höchste Schutzstufe erfordern) zu erstellen.

Bei Häfen muss darauf hingewiesen werden, dass in einigen von ihnen eine wachsende Anzahl von industriellen Steuerungs- und Kontrollsystemen (Industrial Control System – ICS) zu beobachten ist, darunter auch Systeme zur Überwachung, Steuerung und Datenerfassung (Supervisory Control and Data Acquisition – SCADA), über die Industriesysteme und -maschinen mit Netzwerken verknüpft sind, damit sie aus der Ferne oder von Land aus bedient werden können.

Paris, Frankreich - Seine

Selbst wenn diese mechanischen Anlagen nicht per se eine direkte Zielscheibe für Cyberangriffe darstellen, sind sie trotzdem über ihre Vernetzung zugänglich und laufen auf Altsystemen, die von den Anbietern nicht länger aktualisiert werden. So können ICS als Zugangspunkte für Angriffe auf andere Assets benutzt werden. Deshalb lohnt es sich, diese in die Liste der kritischen Assets aufzunehmen.

Die untenstehende Liste beschreibt die wichtigsten Hafenassets und einige Assets in Verbindung mit Schiffen, insbesondere diejenigen, die zu einem bestimmten Zeitpunkt mit den Systemen des Hafens verbunden sein können.



Die wichtigsten Hafenassets

Anlagen zur Schiffsabfertigung und Anleger
Assets in Verbindung mit dem Einlaufen und Anlegen des Schiffes im Hafen. In diesem Zusammenhang zu nennen wären Fluss-Infrastruktursysteme wie das Schleusen- und Brückenmanagement (Lock and Bridge Management – LBM), Sensoren und Mechanismen an verbundenen Torsystemen, Verkehrsmanagementsysteme.

Systeme für Fahrgastschiffe und Tagesausflugsschiffe
Webanwendungen für Buchungssysteme und Ticketverkauf für Fahrgastschiffe sind wichtige geschäftliche Assets für touristische Häfen und als nach außen gerichtete, für die Öffentlichkeit bestimmte Anwendungen besonders anfällig. Gibt es keinen Zugang mehr zu diesen Systemen, könnte der touristische Betrieb unterbrochen oder ausgesetzt werden, was erhebliche Verluste für mit dem Hafen verbundene Firmen oder Geschäftspartner nach sich ziehen kann.

Liegestellen
Tools und Prozesse, die die Versorgung von Schiffen ermöglichen, wie Bunkern von Kraftstoff, Erneuern von Lebensmittelvorräten, Auffüllen von Wassertanks, Durchführung von Schiffsreparaturen usw.

Energiedienste
IT-Tools für das Management und IT-Anwendungen zur Überwachung und Steuerung von Versorgungsleitungen, -ausrüstung, -anlagen und Stromnetzen, die für die Energieversorgung des Hafens und seiner Infrastruktur erforderlich sind.

Sicherheit und Gefahrenabwehr
Alle Tools, die bei der physischen Standortsicherheit von Häfen eine Rolle spielen, wie verbundene Gates, CCTV-Kameradienste, verbundene Türen und Durchgänge, Badgingsysteme, verbundene Alarmsysteme, Wächterposten.

Am Verkehrsmanagement beteiligte IT-Systeme wie Schiffsverkehrsdienste (Vessel Traffic Service – VTS)
Die Verkehrsleitzentralen der Häfen, die für deren Betrieb eine zentrale Bedeutung haben und von der Zuverlässigkeit der Internet- oder UKW-Funkverbindungen abhängig sein können, was sie zu einer potenziellen Zielscheibe von Cyberangriffen macht.

Automatic Identification System (AIS)
System für den automatisierten Austausch von Meldungen zwischen Schiffen über UKW-Funk, das es Schiffen und Verkehrsüberwachungssystemen ermöglicht, die Identität, den Status, die Position und die Route der im Fahrtgebiet befindlichen Schiffe zu erkennen.

Containerlagerung und -sicherung
Ladungs- und Flottenmanagement (Cargo and fleet management – CFM), Tools für das Entladen und die Lagerung von Containern wie zum Beispiel Software für Bewegung, Lagerung und Handling von Containern, Tools für die automatische Sortierung und Handling von Schüttgut, Lagerungs- und Überwachungstools von Kühlcontainern usw.

Behörden und Zoll
Tools zur Anmeldung und Bewertung von Waren für Zollabgaben und Hafengelder, zur Koordinierung der Zollabfertigung, für die Ausgabe von Zollerklärungsformularen, für an öffentliche Stellen gerichtete Anträge und deren Beantwortung.

Supportservice
IT-Hardware, Software und Anwendungen für Häfen, Kommunikationssysteme für das Hafenpersonal, Anwendungen für Immobilien- und Facility-Management sowie für Gefahrgut- und Kühlmanagement. Zu den Supportservice-Assets zählen außerdem die „Systeme für Fahrgastschiffe und Tagesausflugsschiffe“ (siehe spezifische Begriffsbestimmung).

Distributionsdienstleistungen
Vernetzte Tools für die Distribution von Containern oder Schüttgut an die Rangierbahnhöfe, Verkehrshubs, deren Systeme auch Zusatzleistungen wie Containerkontrolle bieten, oder Kommunikationsplattformen für die Containerdistribution. Dazu gerechnet werden ebenfalls verbundene Tools, wie man sie von Bahnhöfen und ihrer Umgebung kennt, sowie die Waggons für den Transport von Containern.

Schiffsassets

Hinweis

Mit Ausnahme der für die Kommunikation zwischen Schiff und Hafen eingesetzten Assets wird davon ausgegangen, dass die schiffsseitigen Assets selbst nicht in den Anwendungsbereich dieses Leitfadens fallen.

River Information Services (RIS)
Schiffsverfolgung und Aufspürung in der Binnenschifffahrt (Inland AIS), Elektronisches Kartendarstellungs- und Informationssystem für die Binnenschifffahrt (Inland Electronic Chart Display and Information System – Inland ECDIS), Nachrichten für die Binnenschifffahrt (Notices to Skippers for Inland Navigation – NtS), Systeme für das elektronische Melden in der Binnenschifffahrt (Electronic Ship Reporting in Inland Navigation – ERI).

Maschinen
Elektronische Geräte für den Schiffsbetrieb, einschließlich für die Antriebmaschinen und anlagen, Leistungsregelungssysteme, Steuerhaussysteme, Kraftstoff-, Batterie- und Ladungssysteme.

Assets für den Geschäftsbetrieb
IT-Assets für die Abwicklung von Geschäftsprozessen an Bord und außerhalb des Schiffes, einschließlich PCs, Laptops, Tablets und ihre Business-Anwendungen.

Kommunikations- und Besatzungstechnologie
Funk-, Satellitenkommunikations- und andere mit dem Land vernetzte Geräte für die Verbindung zwischen Schiff und Land; Mobiltelefone der Besatzung, an Bord und außerhalb des Schiffes benutzte Computer und Tablets.

Ladung
Tools zur Kommunikation über den Status der Ladung sowohl an Bord als auch an Land, in Bezug auf Lieferung, Inhalt und Art der Ladung.

Taxonomie der Bedrohungen für Häfen

Sobald wir die Liste der kritischen Assets bzw. der kritischen Systeme eines Hafens erstellt haben, an denen beim einem Cyberangriff Schäden entstehen können, können wir uns mit den Arten von Bedrohungen beschäftigen, denen diese Assets ausgesetzt sind.

Unter „Bedrohungen für die Cybersicherheit" versteht man Situationen oder Ereignisse mit dem Potenzial, organisatorische Abläufe oder Assets, Personen, andere Organisationen oder den Staat zu schädigen. Dies kann beispielsweise durch unbefugten Zugriff, Zerstörung, Offenlegung, Änderung von Information, und/oder Denial-of-Service erfolgen. Eine Bedrohung kann identifiziert werden, indem die Anfälligkeit eines Hafens mit den Motiven böswilliger Akteure korreliert wird.

Für die Einstufung einer Bedrohung müssen wir damit beginnen, die Arten von Cybersicherheitsattributen aufzulisten, die ein Asset aufweisen muss. Grundattribute der Cybersicherheit sind Vertraulichkeit, Verfügbarkeit und Integrität (allgemein bekannt als „CIA-Triade" - Confidentiality, Integrity, Availability).

Im Zusammenhang mit Binnenhäfen und -schiffen wird noch der Begriff **„Possession"**[5] hinzugefügt.

Die nachfolgende Tabelle beschreibt die vier Hauptattribute, wenn sie auf das Ökosystem Hafen angewandt werden.

Cybersicherheits-Attribute

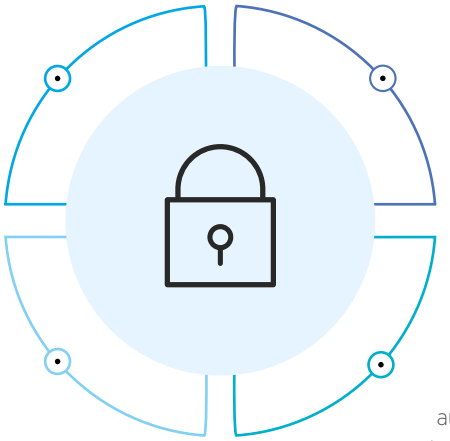
Vertraulichkeit

Daten und Informationen, die unter den vernetzten Hafen-Assets ausgetauscht werden, werden je nach Situation als vertrauliche Daten behandelt. Unbefugte Benutzer haben keine Möglichkeit, auf diese Informationen zuzugreifen, sie herunterzuladen oder zu übertragen.

Possession

Die operative Kontrolle über Hafen- und Schiffs-Assets ist auf befugte Personen beschränkt. Die Fähigkeit, die Kontrolle über Schiffe, Maschinen und andere verbundene Geräte aufrechtzuerhalten, stellt ein Schlüsselattribut für Häfen und Schiffe dar. Die unbefugte Übernahme der Kontrolle über ein Schiffsystem oder ein zentrales Betriebsmittel stellt ein Bedrohungsszenario dar, das genauso Anlass zu Besorgnis geben muss wie die weiter unten beschriebenen Szenarien.

Possession unterscheidet sich von Integrität dadurch, dass der Begriff sich auf den materiellen (im Gegensatz zum virtuellen) Besitz oder auf die Kontrolle bezieht. Im Vergleich zu anderen Umgebungen, die nur über IT-Assets verfügen, sind in Binnenhäfen IT- mit OT-Assets (Operational Technology – Betriebstechnologie) verbunden, damit physische und digitale Dienste in Kombination angeboten werden können. Über solche materiellen Dienste können bei Missbrauch Schäden angerichtet werden, die schlimmer sind als alle finanziellen und rufschädigenden Auswirkungen, und sogar Körperverletzungen und Verlust von Menschenleben zur Folge haben.



Verfügbarkeit

Die für den Betrieb von Häfen oder Schiffen erforderlichen Informationen, Anwendungen, Instrumente und Geräte sind verfügbar, sicher in der Anwendung und belastbar gegenüber potenziellen Störungen.

Integrität

Die für den Betrieb von Binnenhäfen oder Schiffen erforderlichen Informationen, Anwendungen, Instrumente und Geräte bieten präzise, authentische Informationen, die auf dem Weg vom Sender zum Empfänger nicht verändert wurden. Dazu zählt auch die Zusicherung der Nichtabstreitbarkeit, d. h., dass eine Kommunikation Dritten gegenüber nicht von einer der beteiligten Einheiten abgestritten werden kann.

[5] Der Begriff „Possession" wurde hinzugefügt, um dem Praxisleitfaden der Institution of Engineering and Technology mit dem Titel „Cyber Security for Ports and Port Systems" (2020) Rechnung zu tragen.

Mögliche Bedrohungsakteure

Bedrohungsakteure im Bereich der Cybersicherheit können absichtlich oder unabsichtlich Schäden an digitalen Systemen oder Netzwerken verursachen. Dieser Leitfaden konzentriert sich auf die Hauptbedrohungsakteure, die sich in sieben Kategorien unterteilen lassen:

Art des Akteurs	Vorgehensweise	Passwort
Böswillige oder unzureichend geschulte Mitarbeitende	Diese Bedrohungsakteure haben kein Bewusstsein für die richtige Cyber-Hygiene. Sie können aus böswilliger Absicht handeln oder nicht. Ihr Verhalten kann jedoch in jedem Fall ihre Organisation in Gefahr bringen, sei es vorsätzlich oder schlicht durch Nachlässigkeit.	Das Klicken auf einen nicht überprüften Link in einer E-Mail eines Angreifers kann zum Herunterladen von Schadprogrammen führen, die in das IT-System eines Hafens eindringen.
Kriminelle	Motiviert durch finanzielles Gewinnstreben begehen diese Akteure Taten wie Diebstahl, Warenschmuggel, Schleusung von Menschen, Steuerhinterziehung, mutwillige Beschädigung.	Abfangen von Nachrichten, um Container zu stehlen oder zu schmuggeln, ohne Zollabgaben zu zahlen, Diebstahl von Ladung an Bord eines Schiffes, Ransomware zum Einfrieren von IT-Assets mit dem Ziel, Lösegeld zu fordern.
Wettbewerber	Motiviert durch den Wunsch, Geschäfts- oder Marktinformationen zu erhalten, versuchen diese Akteure Informationen abzufangen, die ihnen einen wirtschaftlichen Wettbewerbsvorsprung gewähren.	Gewinnen von vertraulichen Informationen zu Abläufen des Hafenmanagements, um sie für die eigene Geschäftsentwicklung zu nutzen.
Aktivisten oder „Hacktivisten"	Motiviert durch zivilen Ungehorsam verwenden diese Akteure das Internet, um ihre Ideale in der Öffentlichkeit bekannt zu machen oder Druck auszuüben, um ihre Sache durchzusetzen.	Steuerung eines Schiffes, um damit zu Protestzwecken eine Hafeneinfahrt zu blockieren; Manipulation von Infrastrukturbauwerken der Binnenschifffahrt (Brücke, Schleuse usw.), um Störungen im System zu erzeugen.
Nationalstaaten	Akteure, die im Auftrag eines Staates oder einer anderen souveränen Regierungsstruktur handeln, sind durch den Wunsch motiviert, eine Form des (erklärten oder nicht erklärten) Kriegs zu führen, indem sie Störungen hervorrufen oder die Aktivität zum Stillstand bringen.	Durchführung von Denial-of-Service-Angriffen auf Hafen-Assets wie Schleusen, um den Zugang zu einem Fluss oder Gewässer zu blockieren.
Terroristen	Das Internet wird genutzt, um Angst und Schrecken zu verbreiten oder verschiedene Formen von materiellem oder wirtschaftlichem Chaos zu verursachen.	Übernahme der Kontrolle über ein Schiff, um in einem Hafen Schäden und Opfer zu verursachen; Abfangen von Information über die Ankunft von Gefahrgut im Hafen und Einsatz des Gefahrguts, um Chaos zu verbreiten.
Personen, die einer Spionagetätigkeit nachgehen	Ansetzen von Schadprogrammen auf vernetzte Geräte, um geheime oder sensible Daten zu erhalten, die weiterverkauft oder von Informanten verwendet werden können. Die Spionagetätigkeit kann im Auftrag von anderen Staaten oder Wettbewerbern erfolgen.	Andere Staaten erhalten Informationen über einen Transit von sensibler Ladung in einem Hafen (beispiels-weise Impfstoff, medizinische Ausrüstung); Ausspionieren von Abläufen im Hafen, um Wettbewerbsinformationen zu erlangen.

Bei einigen Beispielen aus der obenstehenden Tabelle, wie der Bedrohung durch Terroristen, handelt es sich um Bedrohungen von außen, die nicht in den Anwendungsbereich dieses Leitfadens fallen, da die Häfen selbst keine wirksamen Maßnahmen zur Begrenzung dieser Risiken ergreifen können. Nichtsdestoweniger müssen diese Bedrohungen im Rahmen der Koordination der Cybersicherheit zwischen den Häfen und den anderen Binnenschifffahrtsbeteiligten berücksichtigt werden.

Es muss festgehalten werden, dass die oben genannten Akteure nicht nur aus unterschiedlichen Gründen handeln, sondern auch über unterschiedliche Mittel verfügen und nicht alle die gleiche Hartnäckigkeit mitbringen. Akteure mit Verbindung zu Staaten, die Kampagnen zur Kriegsführung und Spionage durchführen, können über weitreichende Ressourcen verfügen. Tatsächlich lässt sich ein Anstieg von staatlich unterstützen Hackerangriffen verzeichnen, wie ENISA in einer neueren Studie feststellt, die einen Überblick über die Trends in der Cyberspionage bietet[6]. Diese Studie aus dem Jahr 2020 kommt zu dem Schluss, dass ca. 38 % der Bedrohungsakteure mit böswilliger Absicht Verbindungen zur staatlichen Ebene haben und dass 11,2 % der Cyberangriffe auf Cyber-Spionage zurückzuführen sind.

[6] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage

Diese Studie hebt die Risiken hervor, die auf Plattformen für den Umschlag von Rohstoffen lasten. Auch wenn Binnenhäfen in dieser Aufzählung nicht ausdrücklich genannt werden, entsprechen sie dieser Beschreibung und spielen oft eine entscheidende Rolle für die Wirtschaftstätigkeit eines Staates. In diesem Zusammenhang weist die Studie darauf hin, dass staatlich unterstütze Angriffe zunehmen, insbesondere auf öffentliche Versorgungsstrukturen sowie die Sektoren Erdgas, Erdöl und herstellende Industrie. Diese Art von Bedrohungen, die von Staaten unterstützt werden, sollten nicht unterschätzt werden, da es sich hierbei um finanziell gut ausgestattete und von hochqualifiziertem Personal durchgeführte Kampagnen handelt, die unerbittlich ihre hochgradig schädlichen Ziele verfolgen.

Bedrohungstaxonomie

Anhand der Attribute der oben genannten Bedrohungsakteure lassen sich eine Reihe von Bedrohungsszenarien definieren. Auf deren Grundlage lässt sich eine sogenannte Bedrohungstaxonomie für Häfen bzw. eine Liste der Bedrohungen erstellen, für die Häfen, abhängig von ihrer jeweiligen Charakteristik, anfällig sein können.

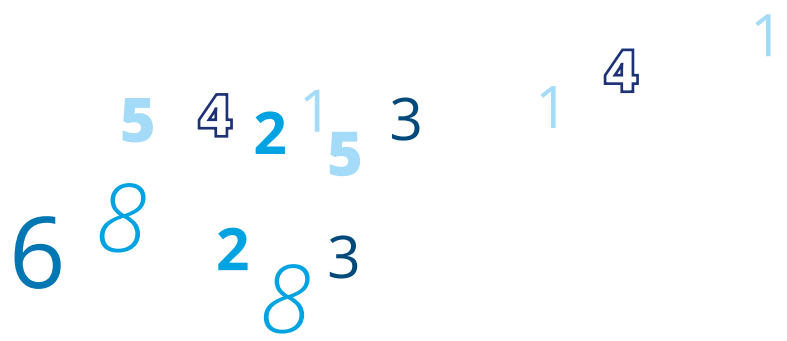
Eine Bedrohungstaxonomie ist ein Mittel zur Analyse von Cybersicherheits-Vorfällen, die potenzielle Auswirkungen haben können. Nach Durchsicht der existierenden Literatur über Bedrohungen für Seeschiffe und Seehäfen konnten die folgenden Bedrohungsarten identifiziert werden. Diese wurden entsprechend angepasst und auf das Ökosystem Binnenhafen übertragen.

	Übertragung auf Binnenhäfen	Beispiel
	Ausfälle, Störungen Für den Hafenbetrieb notwendige Systeme oder Geräte werden beeinträchtigt und können nicht wie erforderlich funktionieren.	Ein Schleusen- oder Brückenmanagementsystem wird durch einen Denial-of-Service-Angriff beeinträchtigt, der zum Einfrieren des Betriebs und damit zur Unterbrechung des Schleusen- oder Brückenbetriebs führt.
	Physische Angriffe Ein Cyberangriff wird gegen ein System für den technischen Betrieb (OT-System) gerichtet, was die physische Übernahme einer Maschine zum Zweck von Betrug, Sabotage, Vandalismus, Diebstahl, Terrorismus, Hacktivismus oder unbefugtem Zugriff/Zugang zur Folge hat.	Ein Schiffsmaschinensystem wird im Rahmen einer fortgeschrittenen andauernden Bedrohung (APT- Advanced Persistent Threat) übernommen und das Schiff wird zu terroristischen Zwecken in einen Hafen gesteuert.
	Abhören, Abfangen, Hijacking Böswillige Eingriffe in das Netzwerk dienen dem Abfangen von sensiblen Daten und des Netzwerkverkehrs oder dem Hijacking einer User-Session.	In einer Container-Management-Anwendung fangen Terroristen gespeicherte Daten mit Informationen über Container mit Gefahrgut ab, um diese an sich zu bringen.
	Spoofing oder Jamming von Informationen Vortäuschung des Ursprungs einer Kommunikation oder eines Datenpunktes (Absender einer SMS, GPS-Position), um den Eindruck zu erwecken, diese kämen von einer bekannten, vertrauenswürdigen Informationsquelle, während es sich in der Realität um Informationen handelt, die vom Angreifer verändert oder erzeugt wurden.	GPS-Information wird gespooft, um falsche Ortsangaben zu vermitteln, wodurch ein Risiko für die Schifffahrt entsteht.
	Katastrophe Ein Cyberangriff auf verbundene Assets des Hafens löst durch die Ausnutzung einer Schwachstelle im Hafen-Ökosystem eine Umwelt- oder Naturkatastrophe aus.	Ein Hacker manipuliert die Daten einer Anwendung zum Container-Management, was den unsachgemäßen Umgang mit Gefahrgutcontainern zur Folge hat. Der dadurch entstandene Brand im Hafen verursacht wiederum schwerwiegende materielle Schäden an den Hafenanlagen.
	Ausfälle Die Versorgung des Hafens mit für den Betrieb notwendigen Ressourcen wird unterbrochen. Zu den Ressourcen zählen beispielsweise Netzwerke, Personal, Kraftstoff, Wasser oder elektrischer Strom.	Ein großflächiger Angriff auf ein angeschlossenes Stromnetz führt zu einem größeren Stromausfall und dem Einfrieren des Hafenbetriebs, sodass der Güterumschlag verzögert wird.
	Unabsichtliche Schädigung Durch den unbeabsichtigten Fehler eines Mitarbeitenden entsteht Schaden an Daten, Systemen oder der materiellen Infrastruktur des Hafens.	Ein Mitarbeitender lädt eine Ransomware-Datei herunter, die die gesamten IT-Systeme des Hafens einfriert. Auf dem gesperrten Bildschirm erscheint eine Lösegeldforderung.

Mögliche Auswirkungen

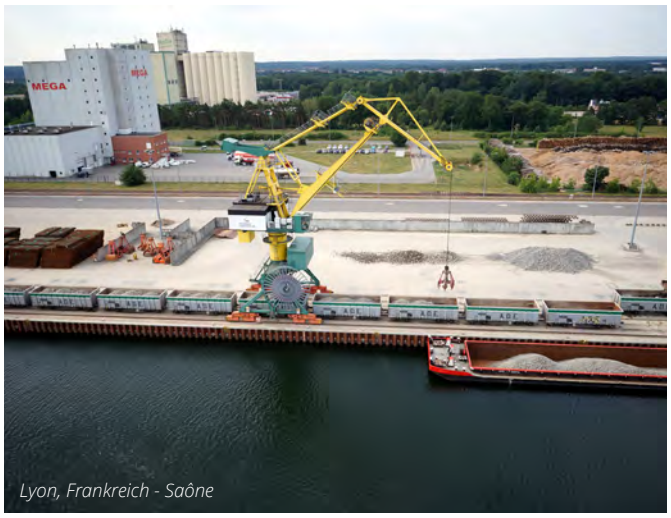
Bedrohungen werden als „beunruhigend" empfunden, weil sie das Potenzial haben, durch ihre Umsetzung einer Organisation reale Schäden zuzufügen. Die weiter oben beschriebenen Attribute der Cybersicherheit können bei Nichtbeachtung entsprechende Auswirkungen auf den Hafen oder dessen Geschäftspartner haben. Ein Cyberangriff kann bei einer Organisation verschiedenste Formen von Schäden nach sich ziehen. Im Folgenden findet sich eine Liste von möglichen Auswirkungen einer Umsetzung von Cybersicherheits-Bedrohungen.

Art der Auswirkung	Beschreibung
Rufschädigung	Eine Cybersicherheitsverletzung oder ein Cybersicherheitsvorfall können langanhaltende Rufschädigungen für den Namen oder die Marke einer Organisation (Hafen, Transportunternehmen, Schiffsbetreiber) nach sich ziehen. Die so entstandenen Schäden lassen sich nur schwer berechnen, da sie oft immaterieller Natur sind, aber zahlreiche Nebeneffekte wie beispielsweise Ausgaben zur Wiedererlangung des Vertrauens der Kundschaft, eine verstärkte behördliche Kontrolle und entgangene Geschäfte haben.
Finanzielle Verluste	Es gibt zahlreiche Kosten, die einer Organisation infolge eines Cybervorfalls entstehen können, beispielsweise für die Wiederherstellung und das Krisenmanagement nach einer Katastrophe, Anwaltsgebühren, Erhöhung von Versicherungsprämien, Warenverluste und Kosten durch die Verzögerungen bei Hafendiensten.
Rechtliche Sanktionen	Ein Cybersicherheitsvorfall kann zu behördlichen Sanktionen wie Bußgeldern und Maßnahmen zur Verschärfung der Rechenschaftspflicht für die betreffende Organisation führen.
Zerstörung von Eigentum	Ein Angriff auf die IT-Systeme eines Hafens kann zur Zerstörung von digitalem Eigentum wie Daten und Informationen führen, wenn diese nicht ordnungsgemäß gesichert werden. Außerdem kann es die Zerstörung von materiellem Eigentum wie IT-Hardware, aber auch von SCADA-Systemen und, als Ergebnis eines erfolgreichen Angriffs, von Hafenfahrzeugen, Maschinen für den Hafenbetrieb, Containern und deren Inhalt zur Folge haben.
Köperverletzung und Verlust von Menschenleben	Ein Cyberangriff mit terroristischer Zielsetzung kann zu Körperverletzung oder gar Verlust von Menschenleben, oder zu einer durch ein gestörtes Schleusensystem verursachte Überflutung führen. Gefahrenstoffe können eine Explosion auslösen.
Kriminelle Aktivitäten: Betrug, illegaler Handel	Kriminelle können Cyberangriffstechniken, wie das Abfangen von Informationen in Netzwerken, dazu nutzen, rechtswidrigen Aktivitäten wie dem Handel mit illegalen Substanzen in Containern oder Menschenhandel nachzugehen.
Diebstahl	Kriminelle können Cyberangriffstechniken mit dem Ziel anwenden, im Hafen befindliche Objekte zu stehlen: Container, deren Inhalt, Waren oder Material (Maschinen, Fahrzeuge, Ersatzteile usw.).
Umweltkatastrophen	Ein Cybersicherheitsvorfall könnte den falschen Umgang mit gefährlichen Stoffen in Containern oder Kraftstoffen zur Folge haben und zu einer Umweltkatastrophe auf Binnenwasserstraßen führen.



Beispiele für Szenarien von Angriffen auf Häfen

Stellvertretend für eine Auswahl aus den weiter oben beschriebenen Angriffsszenarien möchte dieser Leitfaden drei Beispiele mit unterschiedlichen Beweggründen und Akteuren herausgreifen. Ziel dieser Übersicht ist es, greifbare Beispiele dafür zu liefern, wie die oben beschriebenen Assets bedroht werden können. Jedes Angriffsszenario beruht auf einem realen Sicherheitsvorfall aus den letzten Jahren und ist auf das Hafen-Ökosystem anwendbar.



Lyon, Frankreich - Saône

Wijk bij Duurstede, Niederlande - Amsterdam-Rhein-Kanal

Szenario 1

Infiltration von Steuerungssystemen für Maschinen

2013 drangen zwei Hacker in das Steuerungssystem eines kleinen Hochwasserdamms im Bundesstaat New York[7] ein. Der Damm, der vor bei Unwetter entstehendem Hochwasser schützen soll, war durch ein SCADA-System gesteuert, das über ein Mobilfunkmodem direkt mit dem Internet verbunden war. Das System verwendete diese Internetverbindung zur Übermittlung von Status- und Betriebsdaten (Wasserstand u. ä.). Dies gestattete die Fernbedienung des Torsystems, das wiederum das Management der Wasserstände und Durchflussmengen ermöglichte. Es gelang den Hackern nicht, die Torsteuerung in Gang zu setzen, weil die Tore glücklicherweise gerade zu Wartungszwecken vom System abgekoppelt waren. Dieses Angriffsszenario illustriert, wie typischerweise kritische Betriebsabläufe wie die Bedienung von Schleusenanlagen in einem Hafen gestört oder gekapert werden können. Ein solcher Angriff könnte erhebliche Folgen für die Navigationssicherheit und die gewerbliche Tätigkeit haben.

Dieses Angriffsszenario könnte nachgeahmt und auf Hafenanlagen wie das interne Stromversorgungsnetz, Kläranlagen, die Bedienung von Schleusenanlagen, usw. übertragen werden.

[7] https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

Die Hauptphasen von Infektionen mit Schadsoftware (Malware) bei Industriesystemen mit der Gefahr einer potenziellen Auslösung, wie oben beschrieben, oder von anderen Angriffsszenarien auf industrielle Steuerungssysteme (Industrial Control System – ICS) werden im Folgenden beschrieben:

Phase 1 – Infiltration

Es gelingt einem Bedrohungsakteur, die verbundenen Systeme eine Industrieanlage zu infizieren. Dies kann über ein externes Gerät wie beispielsweise einen USB-Stick, einen klickbaren Link, eine herunterladbare Datei oder einfach über eine externe Internetseite geschehen. Handelt es sich um einen USB-Stick, erfolgt die Infektion über einen dort gespeicherten ausführbaren Code, der sich über Computernetze verbreiten kann, wenn der Stick in den Computer eingesteckt wird.

Phase 2 – Ausspionieren

Die Schadsoftware bettet sich in die Systeme der Industrieanlage ein und spioniert die Netzwerkkommunikation aus, um Wege zur Vervielfältigung und Ausbreitung zu finden.

Phase 3 – Sabotage der Sicherheitsprozesse

Die Schadsoftware identifiziert Software mit Sicherheitslücken und sogenannte Backdoors (Hintertüren) im System, damit sie Mechanismen außer Kraft setzen kann, die das Auslösen eines eingedrungenen Schadprogramms verhindern oder eine Bedrohung melden sollen. Sie lässt sich jedoch nicht entdecken, weil sie stufenweise Angriffe auf Betriebssysteme und, im Falle eines Hafenstromnetzes, auf speicherprogrammierbare Steuerungen (SPS) des betriebstechnischen Systems durchführt. Eingriffe in die SPS ermöglichen unter Umständen die Durchführung industrieller Funktionen wie die Überwachung des Wasserdrucks oder des pH-Werts durch Sensoren oder sogar das Öffnen und Schließen von Ventilen.

Phase 4 – Ausüben von Kontrolle

Die Schadsoftware führt Befehlscodes zur Modifizierung der ursprünglich vorgesehenen Funktionen des SPS aus, indem sie beispielsweise die Input-Daten oder die interne Programmierung manipuliert. Im Falle einer Schleuse zwischen zwei Hafenbecken könnte die SPS, ausgelöst durch verfälschte Angaben zu den Wasserständen der beiden Becken, den Befehl zum Öffnen der Schleusentore geben und damit eine gefährliche Schleusenöffnung einleiten. Würde der Schadware-Code bei einem der beiden Tore die Funktionen „Öffnen" und „Schließen" vertauschen, könnte das zur Folge haben, dass die Schleusentore auf beiden Seiten gleichzeitig aufgehen.

Phase 5 – Ausführung

Der Hacker missbraucht das System zur Durchführung einer bestimmten Handlung, um ein bestimmtes Ziel zu erreichen. Im oben erwähnten Fall könnte es zum Beispiel geschehen, dass zu einem Zeitpunkt, an dem sich ein großer Verband in der Schleusenkammer befindet, anstatt des oberen Schleusentors das untere geöffnet wird und der Verband gewaltsam stromabwärts mitgerissen wird; dabei könnten durch die gewaltsame Bewegung der Wassermassen Besatzungsmitglieder verletzt werden oder ums Leben kommen, Materialschäden an den Schiffen des Verbands sowie oberhalb und unterhalb der Schleuse entstehen.

Phase 6 – Replizierung

Die Schadsoftware repliziert sich, um weitere Systeme und Geräte anzugreifen. Im Beispiel der Schleuse zwischen zwei Hafenbecken könnte die Malware weitere SPS-Systeme im näheren Umfeld aufspüren und diese zu einer Zielscheibe machen.

Szenario 2

Kompromittieren von Daten zur Erleichterung von illegalem Drogenhandel

2013 verhafteten belgische und niederländische Behörden ein Dutzend Verdächtige bei dem Versuch, über 1000 kg Kokain sowie 1000 kg Heroin in Containern zu schmuggeln, indem sie sich Zugriff auf die Computersysteme des Hafenbetreibers verschafften[8]. In Zusammenarbeit mit Hackern übernahmen die Straftäter die Kontrolle über die Computer des Container-Terminals, um die Container zu kennzeichnen und nachzuverfolgen, in denen sich die illegalen Drogen befinden. Dieser Ansatz, der sich auf Häfen gut anwenden lässt, sieht aus wie folgt:

Namur, Belgien - Maas

Phase 1 - Intrusion (Eindringen ins System)

Der Täter verschickt E-Mails an die Beschäftigten des Container-Terminals, deren Anhänge Malware mit herunterladbaren Dateien enthalten, die es diesen ermöglicht, Spionagesoftware auf den Computern der Beschäftigten zu installieren.

Phase 2 - Kontrolle

Der Täter ergreift die Kontrolle über infizierte Computer und erhält damit Zugriff auf die Containermanagement-Systeme und/oder Datenbanken.

Phase 3 - Überwachung

Die Container, in denen sich die illegalen Drogen befinden, die geschmuggelt werden sollen, werden im System identifiziert und gekennzeichnet, damit ihre Bewegung nachverfolgt werden kann. Die Täter wissen jeweils genau, wo sich die Ladung befindet und wann Kontrollen geplant sind (Frachtkontrollen, Röntgenkontrollen, Inspektionen usw.).

Phase 4 - Wiederauffinden

Die Täter nutzen ihren Zugang zu den Containermanagement-Systemen, um den Standort eines Containers und dessen Anlieferungszeitpunkt auszuwählen. Sie verschaffen sich noch vor den Hafenbehörden Zugang zum Container und können so ihre illegale Drogenlieferung entgegennehmen.

Die wichtigste Erkenntnis aus diesem Ansatz ist, dass die Kontrolle über Anwendungen zum Containermanagement mit dem unbeabsichtigten Fehlverhalten eines Beschäftigten beginnt.
Alle Studien kommen überein, dass Social Engineering und ganz allgemein der menschliche Faktor die Hauptursache für Cybersicherheitsrisiken darstellen, und dieser Faktor im Allgemeinen unterschätzt wird. Die Zahlen sind nicht immer deckungsgleich, aber der menschliche Faktor spielt nach diesen Angaben mindestens in jedem zweiten Fall eine Schlüsselrolle.

Diese Fallstudie zeigt, wie durch das Herunterladen einer Schadware-Datei die Beschäftigten ihre Organisation und ihre Arbeitgeber einem Risiko aussetzen, indem sie kriminellen Handlungen zum Erfolg verhelfen. Nur Fortbildungen und regelmäßige Sensibilisierungsmaßnahmen für das Personal können dazu beitragen, die Auswirkungen des menschlichen Faktors in einer Organisation nach und nach zu reduzieren.

[8] https://www.europol.europa.eu/sites/default/files/documents/cyberbits_04_ocean13.pdf

Szenario 3

Jammen von AIS-Geräten

Ein Inland-AIS-Gerät wird dazu verwendet, über UKW-Funk die Position eines Schiffs zu übermitteln. Darüber hinaus empfangen fest installierte Antennen entlang der Wasserstraßen diese übertragenen Daten und leiten sie an die Verkehrsleitzentralen an Land weiter, die sie für die Erkennung der Verkehrslage und der Position der einzelnen Schiffe nutzen. Da die UKW-Kommunikation nicht verschlüsselt ist und keine Authentifizierung erfordert, ist sie für Cyberbedrohungen sehr anfällig[9].

2017 meldeten mindestens 20 Schiffe auf dem Schwarzen Meer, dass ihr AIS-Gerät ihre Position als 30 km landeinwärts liegend anzeigte[9]. Angesichts der Tatsache, dass der AIS-Sender-Empfänger für die Sicherheit der Navigation eine wichtige Rolle spielt, hatte dieser (mittels Spoofing durchgeführte) Cybersicherheits-Vorfall eine direkte Auswirkung auf die Sicherheit von Schiff und Besatzung. Die Beweggründe können vielfach sein, angefangen bei Terrorismus über Hacktivismus bis hin zu kriminellen Aktivitäten. Die Phasen eines solchen Spoofings ließen sich wie folgt beschreiben:

Budapest, Ungarn - Donau

Phase 1 - Erkundung

Schiffe mit eingeschaltetem AIS-Gerät sind über eine Antenne oder Fernverbindung für die Übertragung von Geolokalisierungsdaten mit einem Unternehmen verbunden. Ein Zugriff auf diese Lokalisierungs- und Positionsangaben kann durch das Abfangen dieser Verbindungs- und Übertragungsinformationen erfolgen.

Phase 2 - Abfangen von Information

Ein Bedrohungsakteur an Land könnte AIS-Signale abfangen und die Schiffsposition anhand der im Internet verfügbaren Informationen nachverfolgen. Der Bedrohungsakteur könnte dann Funksignale mit der Schiffsposition übertragen, um die Empfänger zu verwirren oder einfach das Signal zu jammen/zu blockieren.

Phase 3 - Ausführung

Der Akteur könnte Funksignale nach verschiedenen Aktionsplänen jammen, wie beispielsweise eine falsche Position an das AIS-Gerät senden und damit eine falsche Darstellung der Schiffsposition erzeugen, oder das Schiff daran hindern, eine genaue Position anzugeben. Das stellt eine Gefahr für die Binnenschifffahrt dar.

Dieses Bedrohungsszenario ist für Häfen besonders relevant, da sich das Hafenpersonal auf die vom AIS-Gerät gesendeten Positionsdaten verlässt, um die Navigation im Hafenbereich zu erleichtern und zu managen. Die Hafenbehörden übertragen dank der AIS-Geräte außerdem spezifische Nachrichten. Wird die Verlässlichkeit solcher Systeme beeinträchtigt, hat dies erhebliche Auswirkungen, die über finanzielle Belange und Rufschädigung hinaus sogar zu einer Gefährdung von Menschenleben führen könnten.

[9] https://www.ship-technology.com/features/ship-navigation-risks/

Fallstudie
Social-Engineering-Kampagnen

Wie die oben aufgeführten Beispiele zeigen, kann der menschliche Faktor in ganz unterschiedlichen Szenarien zu bestimmten Zeitpunkten für Angriffszwecke genutzt werden. Cyberkriminelle wissen das und nutzen diese Schwachstelle beinahe systematisch aus, um ihre Ziele zu erreichen.

Cyberkriminelle und Bedrohungsakteure, die versuchen, ein Cybersystem zu infiltrieren, verlassen sich oft auf die Technik des Social Engineering, um an Informationen zu gelangen und die ersten Phasen ihrer Angriffe durchzuführen. Vereinfacht formuliert versteht man unter **Social Engineering** den Prozess, mit dem versucht wird, eine Person durch manipulierte Interaktion dazu zu bringen, Informationen preiszugeben. Im Rahmen dieser Interaktion verwenden Bedrohungsakteure oft psychologische Tricks, um eine Täuschung zu erzielen. Das Ziel einer solchen Social-Engineering-Kampagne könnte darin bestehen, eine Person dazu zu bringen, auf einen Link mit einem Schadprogramm zu klicken, um an vertrauliche Informationen wie Codes, Passwörter und privilegierte Daten zu gelangen. Bisweilen kann Social Engineering in der Realität und nicht nur im virtuellen Raum stattfinden. So kann eine Person beispielsweise versuchen, über Täuschungsmanöver (Fälschungen, Unredlichkeit) Zugang zu einem physischen Standort zu erlangen.

Eine der verbreitetsten Formen von Social-Engineering-Angriffen ist das sogenannte **Phishing**, eine Vorgehensweise, bei der eine Nachricht versendet wird (E-Mail, Telefon, SMS usw.), die eine Art Köder benutzt und an eine (sehr) große Anzahl von Personen in der Hoffnung verschickt wird, dass zumindest einige sich darauf einlassen. Gelingt die Täuschung, kann der Angreifer damit rechnen, entweder einen finanziellen Vorteil oder bestimmte personenbezogene bzw. vertrauliche Daten erschlichen zu haben, die er später für kriminelle Zwecke verwenden kann. Wenn der Angriff auf einen kleineren Personenkreis (manchmal nur eine einzelne Person) gerichtet ist, spricht man von **Spear-Phishing**, wobei in diesem Fall der Köder sehr viel sorgfältiger gewählt und auf die Zielperson zugeschnitten ist, was ihn noch überzeugender macht.

In dieser Fallstudie beschäftigen wir uns genauer mit fünf verbreiteten Phishing-Kampagnen, die Social Engineering nutzen: Manipulation von Links, Smishing, Vishing, Fälschung von Websites und Pop-ups.

Linkmanipulation ist eine Methode, bei der ein Bedrohungsakteur einen Nutzer dazu bringt, eine gefälschte Website anzuklicken. Dies kann mittels einer E-Mail, einer Textnachricht, eines Social-Media-Posts oder über eine andere Austauschplattform geschehen. Die fragliche Website ähnelt in einem solchen Fall einer bekannten und vertrauenswürdigen Quelle, wurde aber für die Zwecke des Bedrohungsakteurs manipuliert.

Smishing ist eine Form von Phishing, bei der versucht wird, unter Einsatz einer Textnachricht (SMS) an private Informationen des Opfers zu gelangen. Die meistverbreiteten Formen von Smishing sind Textnachrichten mit einem Link, der automatisch Schadware herunterlädt. Ist die Schadware einmal installiert, kann sie persönliche Daten wie Berechtigungsinformationen, Bewegungsdaten oder Telefonnummern aus Kontaktlisten stehlen, um das Virus in der Hoffnung auf eine exponentielle Vervielfältigung weiterzuverbreiten. Eine andere Smishing-Taktik besteht darin, sich als legitime und wohlbekannte Institution auszugeben, um von den Opfern persönliche Informationen anzufordern.

Vishing ist eine Form des Telefonbetrugs, oder anders gesagt, eine Form von Phishing über Telefonanrufe, die menschliche Kontakte dazu nutzen, Opfer zu überzeugen, Informationen wie PIN-Nummern, persönliche und private Informationen, Passwörter oder andere personenbezogene Daten preiszugeben. Die Anrufer können sich als Vertreter offizieller Stellen wie Banken oder Regierungsbehörden, aber auch der IT- oder Personalabteilung des Unternehmens (oder des Unternehmenssitzes) oder sogar als Vorgesetzte ausgeben, um das Opfer in Vertrauen zu wiegen und so gewünschten Informationen zu erhalten.

Website-Fälschung funktioniert so, dass sich eine schädliche Website als authentisch darstellt, damit die Besucher ihre sensiblen Informationen wie Kontendetails, Passwörter oder Kreditkartennummern preisgeben.

Pop-up-Meldungen sind intrusive Methoden zur Informationsgewinnung, bei denen Pop-ups auf dem Endgerät des Opfers erscheinen und es auffordern, Informationen einzugeben. Häufig verleitet das Erscheinen eines Pop-ups auf dem Endgerät das Opfer mühelos dazu, Informationen preiszugeben, die an die Bedrohungsakteure übermittelt werden.

Social-Engineering-Techniken, wie oben beschrieben, weisen oft die folgenden Merkmale auf:

1. irreführende Information: URLs sehen häufig etwas anders aus und Mitteilungen per E-Mail/SMS können Rechtschreibfehler aufweisen, da sie in der Regel von Amateuren oder Ausländern mit Hilfe von maschinellen Übersetzungen verfasst werden;
2. verwendung von drängenden Formulierungen: Die Akteure stützen sich auf die Wirkung von Angst und Schrecken, um bei den Opfern Panik zu erzeugen, die sie zur Preisgabe von Informationen verleitet, die sie sonst nicht offenlegen würden;
3. versprechen attraktiver Belohnungen: Anreize wie die Aussicht auf finanziellen Gewinn oder Geschenke sollen die Interaktion mit den Opfern fördern;
4. bitten um vertrauliche Informationen: Bitten um vertrauliche Informationen kommen selten von offiziellen Stellen, sind aber die Grundlage vieler Phishing-Anfragen;
5. verdächtige Anhänge: Im Zusammenhang mit manipulierten Links oder Pop-up-Fenstern können Kriminelle ihre Opfer dazu auffordern, Schadwaredateien auf ihre Endgeräte herunterzuladen;

Sollten Sie eine Phishing-E-Mail oder eine Nachricht erhalten, die verdächtig wirkt, gehen Sie am besten wie folgt vor:

1. klicken Sie auf keinen Fall auf im Dokument enthaltene Links und laden Sie keine angehängten E-Mail-Dateien herunter;
2. markieren Sie die Nachricht als Spam oder als unerwünscht;
3. wenn Sie die Möglichkeit haben, schicken Sie eine Kopie der E-Mail oder einen Screenshot der Adresse aan den Sicherheitsverantwortlichen Ihrer Organisation, damit eine Fachperson über die Situation informiert ist und eventuell weitere Angriffe vereiteln kann.

Im Zusammenhang mit Cybersicherheitsbedrohungen für das Hafenumfeld ist es wichtig zu verstehen, dass die meisten Cyberbedrohungen zu irgendeinem Zeitpunkt ihres Ablaufs auf das menschliche Versagen setzen. Deshalb werden die Techniken des Social Engineering und insbesondere die weiter oben beschriebenen Phishing-Kampagnen weitreichend angewendet und müssen sehr ernst genommen werden. Manchmal reicht ein einzelner Beschäftigter des Unternehmens aus, um der gesamten Organisation Schaden zuzufügen.

In positiver Hinsicht lässt sich aus dieser Fallstudie die Schlussfolgerung ziehen, dass eine gute Sensibilisierung des Hafenpersonals, des Managements, der Lieferanten und anderer dazu „ausreicht“, sich sehr wirksam vor zahlreichen Cyberbedrohungen zu schützen. Es ist einfach, kostengünstig und sehr effizient, wenn alle diese Personen regelmäßig über Social-Engineering-Tricks aufgeklärt und dazu aufgefordert werden, ihren Teil zur Aufrechterhaltung der Sicherheit beizutragen, indem sie wachsam und aufmerksam bleiben.

Teil 2

Minderung von Cybersicherheitsrisiken

Wien, Österreich - Donau

Überblick über Rechtsvorschriften und Politiken in Bezug auf die Situation von Häfen

Gegenwärtig gibt es keine gemeinsamen, verbindlichen Maßnahmen für die Minderung von Cybersicherheitsrisiken, denen Häfen ausgesetzt sind. Dies kann auf die große Vielfalt an Verordnungsgebern zurückgeführt werden, die für den Bereich der Binnenhäfen zuständig sind. Hinzu kommt, dass sich die überwältigende Mehrzahl von Vorschriften mit Seehäfen beschäftigt und nicht spezifisch auf die Situation von Binnenhäfen eingeht. Vor diesem Hintergrund versucht dieser Leitfaden, einen Rahmen für Maßnahmen zur Minderung von Cyberrisiken zu bieten, der die bestehenden Lücken in der aktuellen fragmentierten Literatur und im rechtlichen Umfeld schließen soll.

In diesem Zusammenhang muss zumindest für die EU-Mitgliedsstaaten erwähnt werden, dass auf EU-Ebene eine auch als „NIS-Richtlinie" bekannte Rechtsvorschrift besteht, die das Gesamtniveau der Cybersicherheit in der EU verbessern soll (Richtlinie 2016/1147 des Europäischen Parlaments und des Rates). Diese Richtlinie, die im August 2016 in Kraft trat, enthält Sondervorschriften für besondere Akteure, die als „Betreiber wesentlicher Dienste" identifiziert wurden. Die Beförderungsunternehmen der Binnenschifffahrt werden in der Richtlinie auch wenn es den jeweiligen Mitgliedstaaten obliegt, die Betreiber wesentlicher Dienste zu ermitteln. Den Lesern dieses Leitfadens aus EU-Mitgliedstaaten auf der Suche nach Zusatzinformationen zur Einhaltung dieser Vorschriften wird empfohlen, sich mit den Abschnitten der NIS-Richtlinie vertraut zu machen, die sich auf Betreiber wesentlicher Dienste beziehen, insbesondere wenn die geprüften Binnenhäfen von ihrem Staat als Betreiber wesentlicher Dienste betrachtet werden.

Außerdem werden von einer Reihe nationaler Behörden ebenfalls Ansätze zur Minderung von Cybersicherheitsrisiken für Akteure der Binnenschifffahrt veröffentlicht. Den Lesern dieses Leitfadens wird deshalb empfohlen, sich gleichzeitig mit den in ihrem Staat anwendbaren technischen Vorschriften und Maßnahmen zu deren Einhaltung vertraut zu machen.

Aufbau der Darstellung der Risikominderungsmaßnahmen in diesem Leitfaden

Für die Zwecke dieses Leitfadens wurden Maßnahmen zur Begrenzung der oben beschriebenen eventuellen Risiken für die Cybersicherheit in drei Abschnitte unterteilt:

1. **Organisatorische Strategien und Verfahren (OPP, Organisation Policies and Procedures)**
   In diesem Abschnitt werden Empfehlungen zur Organisationsstruktur, zu Rollen und Verantwortlichkeiten, Gouvernance-Maßnahmen und Organisationsstrategien zusammengefasst, deren Umsetzung den Grad an Cybersicherheit (Cybersicherheitsreife) in einem Hafen verbessern kann.
2. **Informationstechnologische / betriebstechnische Strategien für Häfen**
   Dieser Abschnitt erörtert Strategien, die zur Sicherung von in Teil 1 identifizierten Assets angewendet werden können.
3. **Technische Cybersicherheitsmaßnahmen für Binnenhäfen (TSM, Technical Security Measures)**
   Dieser Abschnitt soll einen allgemeinen Überblick über grundlegende Sicherheitsmaßnahmen bieten, die die IT-Fachkräfte der Binnenhäfen zur Sicherung der IT-Infrastruktur anwenden können.

Zwar können die einzelnen Abschnitte einen allgemeinen Überblick über die Gefahrenabwehrmaßnahmen bieten, die ein Hafen in Betracht ziehen kann, doch sollen sie keinesfalls die Sicherheitsanforderungen ersetzen, die im Rahmen eines Audits oder der Vorschrift eines Zertifizierungsgremiums, eines Staates oder einer anderen Regulierungsbehörde vorgeschrieben werden.

Die hier vorgeschlagenen Risikominderungsmaßnahmen werden in aufsteigender Reihenfolge des Cyberreifegrads aufgeführt. Die zu Beginn jeder der nachfolgenden Tabellen beschriebenen Maßnahmen sollten in einem Ansatz zur Berücksichtigung der Cybersicherheit als erste umgesetzt werden. Im Laufe der schrittweisen Einführung der Maßnahmen und mit wachsender Cybersicherheitsreife können die jeweils darauffolgenden Maßnahmen durchgeführt werden. Zur Erkennung des Reifegrades jeder dieser Maßnahmen wird ein Farbschema verwendet:

- Reifegrad: **niedrig**
- Reifegrad: **mittel**
- Reifegrad: **hoch**

Weitere Informationen zu dieser Einstufung finden Sie im Bewertungsraster in Teil 3.


Meppel, Niederlande - Meppelerdiep

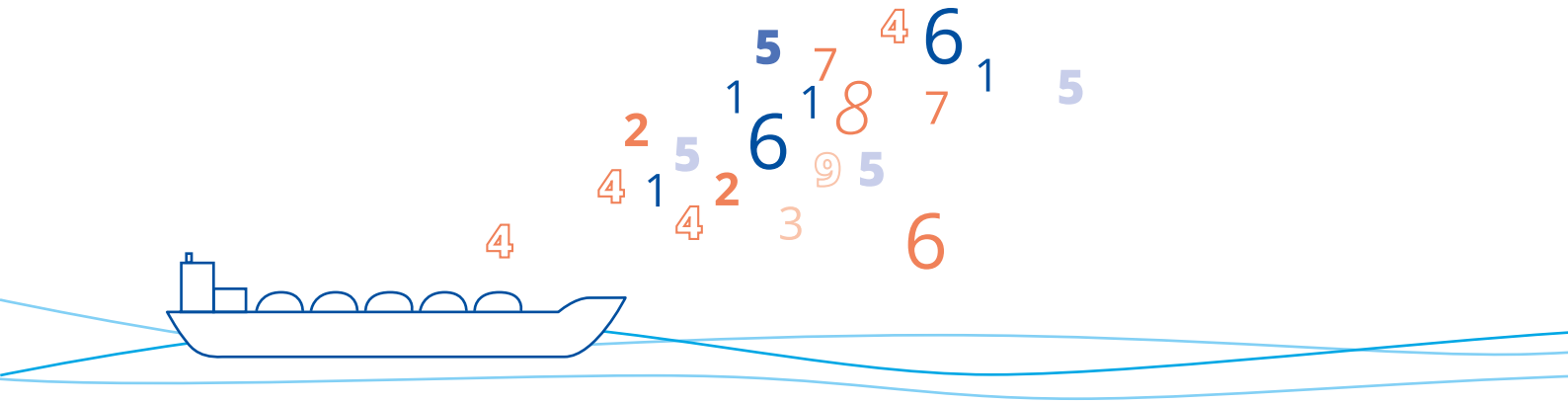
Organisatorische Strategien und Verfahren (Operational Policies and Procedures – OPP)

Dieser Abschnitt liefert einen Überblick über die organisatorischen Strategien und Verfahren, die zum Erreichen einer ausgereiften Cybersicherheitsorganisation umgesetzt werden können. Diese Maßnahmen können durch die obersten Beauftragten für Informationssicherheit des Hafens oder, bei kleineren Binnenhäfen oder Einrichtungen, durch die Direktion oder andere Führungsverantwortliche umgesetzt werden. Sie sind allgemein anwendbar, können sich aber bezüglich ihres Umfangs, ihrer Tiefe und ihres Anwendungsgebiets unterscheiden, je nachdem, welche Ressourcen dem betroffenen Hafen zur Verfügung stehen.

Rollen und Verantwortlichkeiten

Die Zuweisung klarer Rollen und Verantwortlichkeiten bildet den ersten Schritt bei der Einführung einer Rechenschaftspflicht zur Stärkung der Cyberreife einer Organisation. Um diesen Bereich abzudecken, sollten Häfen die folgenden Maßnahmen umsetzen:

	Nummer	Maßnahme
●	[OPP] 1.1	Die Direktion muss Aspekte der Cybersicherheit in ihre Prioritäten mit einbeziehen und angemessene Mittel und Ressourcen für die Umsetzung geeigneter Maßnahmen bereitstellen, wie sie beispielsweise in diesem Leitfaden vorgeschlagen werden. Sie muss zunächst eine offizielle Kontaktperson für sämtliche Cybersicherheitsmaßnahmen bestimmen, und die Kontaktdaten sowie die Rolle dieser Person sollten dem gesamten Personal sowie den Untervertragsnehmern weitreichend kommuniziert werden. Die Direktion muss dabei immer bedenken, dass sie zwar die Umsetzung der Cybersicherheit delegieren kann, nicht aber die Verantwortung für deren Umsetzung.
●●	[OPP] 1.2	Eine allgemeine Charta für Cybersicherheit mit klaren Ansprüchen an alle Mitarbeitenden sollte verfasst und von Personal und Hafenbeteiligten unterzeichnet werden.
●●●	[OPP] 1.3	Eine allgemeine Strategie für Cybersicherheit oder eine Leitlinie für die Sicherheit der Informationssysteme sollte erarbeitet und von der Direktion genehmigt werden.
●●●	[OPP] 1.4	Die Cybersicherheitsstrategie sollte die Rolle eines jeden Hafenbeteiligten klar festlegen (Hafenverwaltung, Terminalbetreiber, Dienstleister, Lieferanten usw.).
●●●	[OPP] 1.5	Alle Sicherheitsaspekte der Partnerschaften mit Dritten sollten definiert und dokumentiert werden, insbesondere bei kritischen Systemen, die von Drittanbietern bereitgestellt werden.
●●●	[OPP] 1.6	Die Cybersicherheitsstrategie sollte regelmäßig überprüft und in der Folge von Risikobewertungen, organisatorischen Neuerungen oder Sicherheitsvorfällen aktualisiert werden.



Organisatorische Prozesse

Sobald die Rollen und Verantwortlichkeiten geklärt sind, geht es in einem zweiten Schritt darum, diese Prozesse und Anforderungen zu dokumentieren, um die Kontinuität dieser Dienste zu gewährleisten, bestimmte Sicherheitsvorschriften zu erfüllen und einen ordnungsgemäßen Informationstransfer im Falle einer Reorganisation der Dienste innerhalb des Hafens sicherzustellen.

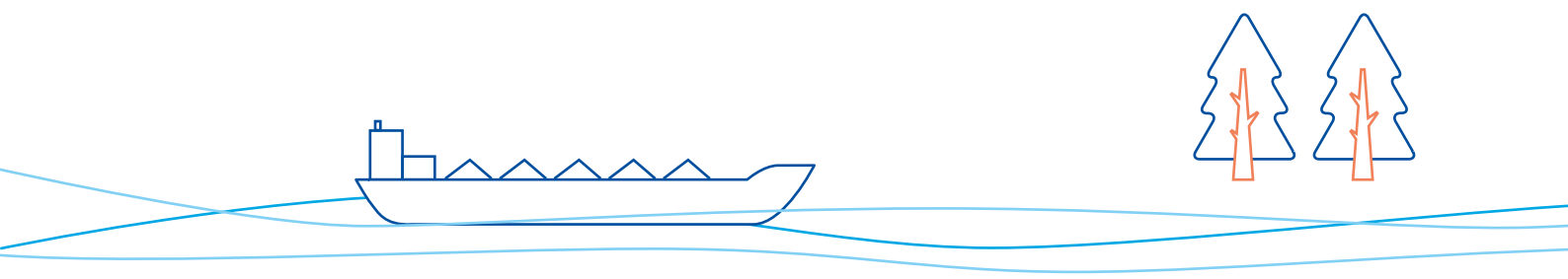
	Nummer	Maßnahme
●	[OPP] 2.1	Eine vollständige Bewertung des Hafens sollte vorgenommen werden, um die zentralen Assets zu ermitteln und eine Rangfolge ihrer Kritikalität zur erstellen.
●	[OPP] 2.2	Die grundlegenden Anforderungen an die Cybersicherheit der betroffenen Lieferanten sollten dokumentiert und den Lieferanten mitgeteilt werden. So könnten beispielsweise Standardklauseln zur Cybersicherheit verfasst und in allen Lieferantenverträgen verwendet werden. Die Einhaltung dieser Anforderungen sollte von sachkundigen Mitarbeitenden des Hafens oder einer vertrauenswürdige Drittpartei überwacht werden, deren ausschließliche Rolle in dieser Überwachung besteht.
●	[OPP] 2.3	Personen in wichtigen Führungspositionen oder mit hoher IT-Verantwortung (Systemadministratoren, IT/OT-Betreiber) sollten vor ihrer Einstellung eine Zuverlässigkeitsüberprüfung durchlaufen. Der Nachweis dieser Prüfung sollte für behördliche Zwecke in den Akten verwahrt werden.
●●	[OPP] 2.4	Auch die Abhängigkeitsverhältnisse und Informationsflüsse bei den oben ermittelten Assets sollten dokumentiert werden.
●●	[OPP] 2.5	Um die mit den einzelnen Assets verbundenen Cybersicherheitsrisiken zu ermitteln, sollte jeweils eine entsprechende Risikobewertung durchgeführt werden. Die Direktion sollte sicherstellen, dass für jedes neue Projekt oder jede neue Initiative eine Bewertung des Cybersicherheitsrisikos erfolgt, insbesondere dort, wo neue Technologien zum Einsatz kommen.
●●●	[OPP] 2.6	Die Hafen-Assets sollten regelmäßig internen und externen Cybersicherheits-Audits und Compliance-Prüfungen unterzogen werden. Dabei muss die Direktion festlegen, wie häufig solche Audits und Compliance-Prüfungen stattfinden müssen. Der Hafen könnte die Automatisierung bestimmter technischer Audits ins Auge fassen, wenn dies möglich ist. Bei Häfen, die eine spezifische Software entwickelt haben, ist es beispielsweise denkbar, mithilfe spezieller Tools regelmäßige Analysen des Quellcodes vorzusehen, um nach eventuellen Schwachstellen oder bekannten Sicherheitslücken zu suchen.
●●●	[OPP] 2.7	Die festgelegten und angewendeten Cybersicherheitsprozesse sollten dokumentiert, validiert und regelmäßig überprüft werden. Die folgenden Themen sollten möglicherweise Gegenstand schriftlich festgehaltener Beschlüsse werden (einschließlich, aber nicht beschränkt auf): • bestehende Cybersicherheitsmaßnahmen zur Sicherung von Webportalen und Webdiensten; • cybersicherheitsmaßnahmen für Netzwerks- oder Kommunikations-verbindungen (einschließlich der Technologien zur drahtlosen Kommunikation); • cybersicherheitsmaßnahmen für das Konfigurieren von Software; • vorschriften und Regeln für Geräteverbindungen mit der IT-Umgebung (einschließlich Verbindungen zu persönlichen Geräten); • maßnahmen zur Aktualisierung von Software und für das Change-Management (bei Verwendung von ITIL); • regeln für die Verwendung von privatem Mobilfunk; • regeln für den angemessenen Umgang mit der Hafen-Infrastruktur durch die Beschäftigten, in Übereinstimmung mit der allgemeinen Cybersicherheits-Charta; • konfiguration und Management der Privilegien von Nutzer- und Systemkonten, einschließlich derjenigen von Drittpersonal mit Zugriff auf die Hafensysteme (wie Energie, Heizung, Elektrizität usw.); • abläufe bei der Bewältigung von Cybersicherheitskrisen und -vorfällen.

Physischer Schutz

Im Zusammenhang mit der Cybersicherheit spricht man von „physischer Sicherheit“, sobald ein physischer Schutz von IT-Ausrüstung erforderlich ist. Oft wird die „physische Sicherheit“ der „logischen Sicherheit“ gegenübergestellt, die darin besteht, die IT-Ausrüstung vor Zugriffen durch Software oder über das Netz zu schützen. Die physische Sicherheit ist jedoch eine eigenständige Dimension der Cybersicherheit, denn sie kann in zahlreichen Angriffsszenarien zum Tragen kommen. Der einfache Zugriff auf einen Ein-/Ausschalter kann ausreichen, um einen Server außer Betrieb zu setzen, ebenso wie der Zugriff auf einen USB-Port das Einschleusen von Schadware unter Umgehung des Netzwerkschutzes ermöglicht. Die physische Sicherheit umfasst auch den Brandschutz und den Schutz vor Überspannungen oder Stromausfällen.

Bei der Ausarbeitung eines Cybersicherheitsplans sollten auch Anforderungen an den physischen Schutz berücksichtigt werden. Kritische IT-Infrastrukturen können Schwachstellen aufweisen, wenn sie für Externe mit möglicherweise schädlichen Absichten zugänglich sind. Deshalb sollten Cybersicherheitspläne auf Risiken eingehen, die sich aus der Verletzung der physischen Sicherheit ergeben.

	Nummer	Maßnahme
●	[OPP] 3.1	Die Direktion sollte klare Regeln für die physische Sicherheit festlegen und Maßnahmen zur Kontrolle des physischen Zugangs anwenden, um Diebstahl, Zugang zu und Beschädigung von sensiblen Hafensystemen zu verhindern. Es sollte eine Liste dieser sensiblen Systeme erstellt und im Vorfeld von der Direktion genehmigt werden.
●	[OPP] 3.2	Über die sensiblen Systeme hinaus sollte der Hafen Versorgungseinrichtungen einschließlich Heizungs, Lüftungs- und Kühlsystemen durch physische Schranken für die physische Zugangskontrolle oder verriegelte Türen vor unbefugtem Zugang schützen.
●	[OPP] 3.3	Jeder genehmigte physische Zugang zum Hafen sollte protokolliert und mindestens einmal jährlich überprüft werden.
●●	[OPP] 3.4	Eine Verfahrensweise für den Fall eines physischen Einbruchs und des Eingreifens durch das Hafenpersonal in diesem Zusammenhang, sowie der für solche Zwischenfälle bereitgestellten Mitarbeitenden externer Agenturen, sollte genauso wie die ergriffenen Abwehrmaßnahmen dokumentiert und notifiziert werden.
●●	[OPP] 3.5	Der Umfang, in welchem bestimmte Bereiche des Hafens Dritten oder der Öffentlichkeit zugänglich sind, sollte dokumentiert und evaluiert werden, um sicherzustellen, dass es sich noch um ein akzeptables Risiko handelt.
●●	[OPP] 3.6	Eine Politik der physischen Zugangskontrolle sollte Schritt-für-Schritt-Verfahren für kritische Sicherheitsvorgänge vorsehen, wie die Rückgabe von Badges durch Mitarbeitende bei ihrem Ausscheiden aus dem Unternehmen, die Aktualisierung von Alarmcodes, die Verwaltung von CCTV-Aufnahmen usw.



Reaktion auf Vorfälle und Krisenmanagement

Für das Eintreten von Cybersicherheitsvorfällen oder krisen sollten klare Vorgehensweisen und Verfahren erarbeitet und umgesetzt werden. Für die Zwecke dieses Leitfadens wird unterschieden zwischen **Cybersicherheitsvorfällen** (d. h. Problemsituationen, die vom IT- oder Sicherheitspersonal ohne Eskalation oder Rücksprache gelöst werden können) und **Cybersicherheitskrisen** (Problemlagen größeren Umfangs, die den Hafenbetrieb beeinträchtigen und das Tätigwerden der Direktion erforderlich machen).

	Nummer	Maßnahme
●	[OPP] 4.1	Der Hafen sollte über einen durch die Direktion genehmigten Plan für das Management von Sicherheitsvorfällen verfügen, der auf Kenntnissen über die in seinem Umfeld möglichen Ursachen von Störungen der Cybersicherheit, der in seiner Liste kritischer Assets aufgeführten wesentlichen Systeme und der Ressourcen und Kapazitäten beruht, die ihm zur Verfügung stehen.
●●	[OPP] 4.2	Der Hafen sollte über einen durch die Direktion genehmigten Krisenmanagementplan verfügen, der die Entscheidungsprozesse detailliert darlegt und den Kommunikationsprozess beschreibt, der bei Störfällen und in solchen Fällen zu respektieren ist, in denen ein Vorfall zu einer Krise eskaliert.
●●	[OPP] 4.3	Der Krisenmanagementplan sollte Angaben zur Berichterstattungspflicht und, wenn anwendbar, zur Zusammenarbeit mit den nationalen Behörden enthalten.
●●	[OPP] 4.4	Der Krisenmanagementplan sollte ein Verfahren zur gegebenenfalls erforderlichen Kommunikation mit von Cybervorfällen betroffenen Parteien und Opfern umfassen.
●●	[OPP] 4.5	Das im Hafen mit dem Vorfallmanagement betraute Personal sollte die Nachrichten des Gewerbes mitverfolgen, um über Sicherheitsvorfälle informiert zu sein, die möglicherweise bei anderen Mitgliedern der Branche aufgetreten sind. Außerdem sollte ein Bedrohungsanalyseverfahren festgelegt werden, um einschlägige Informationen über Sicherheitsbedrohungen für Häfen zu sammeln.
●●	[OPP] 4.6	Der Krisenmanagementplan sollte eine genaue Definition dessen enthalten, was einen Cybersicherheitsvorfall kennzeichnet, welche Rollen und Verantwortlichkeiten sich beim Umgang mit einem Vorfall ergeben und ein Verfahren enthalten, das genau beschreibt, wann aus einem Zwischenfall eine Krise wird.
●●●	[OPP] 4.7	Es sollte ein Plan zur Aufrechterhaltung des Geschäftsbetriebs erarbeitet werden, der sicherstellt, dass der Hafenbetrieb auch bei einem Zwischenfall oder einer Krise fortgesetzt werden kann. Dieser Plan sollte klare Ziele umfassen. Er enthält die Hauptparameter, die für die Aufrechterhaltung des Hafenbetriebs wichtig sind, wie Zeitvorgaben für die Datenwiederherstellung (recovery time objective — RTO), die in Kauf genommene Menge an Datenverlust (recovery point objective – RPO), die maximal hinnehmbare Ausfallzeit (maximum tolerable outage – MTO) und das Minimalziel für die Geschäftskontinuität (minimum business continuity objective – MBCO).
●●●	[OPP] 4.8	Der Krisenmanagementplan sollte eine Analysephase für die Zeit nach dem Zwischenfall vorsehen.
●●●	[OPP] 4.9	Die festgelegten Verfahren zum Umgang mit Vorfällen oder Krisen sollten regelmäßig evaluiert und getestet werden, ggf. anhand von Krisensimulationen oder Tabletop-Analysen. Diese sollten auf eine größtmögliche Anzahl von Beteiligten ausgedehnt werden, damit für die entsprechende Bereitschaft entlang der gesamten Lieferkette gesorgt ist.
●●●	[OPP] 4.10	Nach signifikanten Cybersicherheitsvorfällen (Angriffe von ungewöhnlicher Natur oder mit einer Auswirkung auf den Betrieb) sollte die Direktion sicherstellen, dass diese Vorfälle gemeldet und die diesbezüglichen Informationen verbreitet werden, damit das Gewerbe aus diesen Erfahrungen lernen kann.
●●●	[OPP] 4.11	Der Hafen könnte die Einrichtung eines Security Operations Centre (SOC) für die Verbesserung der Cybersicherheit und das Management von Cybervorfällen in Betracht ziehen.

Cybersicherheitspläne: Im Rahmen der oben aufgeführten Maßnahmen wird auf verschiedene Unterlagen in Verbindung mit der Cybersicherheit eingegangen, die unabhängig betrachtet werden können, aber letztendlich eine kohärente Gesamtheit bilden:

- vorfallmanagementplan;
- krisenmanagementplan;
- plan für die Aufrechterhaltung der Tätigkeit.

Die „Sicherheitsleitlinien“ sind ein weiteres Dokument (auf das bei den höheren Reifegraden der weiter oben dargestellten „Rollen und Verantwortlichkeiten“ eingegangen wird), das einen Teil enthält, der erklärt, wie die verschiedenen Pläne umzusetzen, zu überarbeiten und zu testen sind.

Schulungen und Sensibilisierung

Für die Verbreitung bewährter Verfahrensweisen im Bereich der Cybersicherheit sind Schulungen und Sensibilisierungsmaßnahmen für alle Akteure der Binnenhäfen von entscheidender Bedeutung. Wie bereits an anderer Stelle erklärt, ist das Ausnutzen des „Faktors Mensch“ durch Cyberkriminelle die Voraussetzung für den Erfolg der meisten Angriffsszenarien. Die folgenden Maßnahmen können dazu beitragen, das durch den menschlichen Faktor bedingte Risiko zu mindern, indem man Beschäftigte über die wichtige Rolle aufklärt, die ihnen bei der Gewährleistung der Cybersicherheit zukommt.

	Nummer	Maßnahme
○	[OPP] 5.1	Beschäftigte sollten dahingehend sensibilisiert werden, sorgfältig mit E-Mails umzugehen. Dabei sollten die folgenden Punkte unterstrichen werden: • Die Identität des Absenders muss überprüft werden; • Anhänge und Internet-Links mit verdächtigem oder unbekanntem Absender dürfen nicht geöffnet werden.
○	[OPP] 5.2	Der Hafen sollte Leitlinien für die Verwaltung von Passwörtern festlegen. Diese Leitlinien sollten eine pädagogische Dimension beinhalten, mit der das Personal für die Verwendung starker Passwörter sensibilisiert wird. Sie müssen auch die Regeln für die Erneuerung von Passwörtern umfassen. Im Rahmen dieser Leitlinien sollte zwischen individuellen Benutzerpasswörtern und Passwörtern für System- oder Administratorenkonten unterschieden werden, die aus dienstlichen Gründen gemeinsam genutzt oder von Programmen verwendet werden können.
○	[OPP] 5.3	Beschäftigte sollten über einen ordnungsgemäßen Umgang mit sozialen Netzwerken, Foren, Formularen usw. aufgeklärt werden, besonders, wenn sie mit den Hafen betreffenden Informationen umgehen.
○	[OPP] 5.4	Beschäftigte sollten bezüglich der Installation von Programmen und Software sensibilisiert werden. Die Anforderungen an die Genehmigung für das Herunterladen von Software durch die Hafenadministratoren sollten ausdrücklich kommuniziert werden.
○	[OPP] 5.5	Beschäftigte sollten hinsichtlich der Nutzung von Wi-Fi, 4G/5G und sicheren Netzwerken sensibilisiert werden: Bei Geschäftsreisen sollten sie bei der Nutzung von öffentlichen Wi-Fi-Netzen Vorsicht walten lassen.
○	[OPP] 5.6	Für die Beschäftigten sollten Grundsätze für die Trennung zwischen privater und beruflicher Nutzung von Endgeräten sowie für das Arbeiten mit ihren eigenen privaten Endgeräten (BYOD) erstellt und wirksam kommuniziert werden.
○	[OPP] 5.7	Der Hafen sollte ein regelmäßig wiederkehrendes Sensibilisierungsprogramm zur Cybersicherheit für alle Beschäftigten ausarbeiten, das die allgemeinen Grundlagen der „Cyberhygiene“ behandelt.
●●●	**[OPP] 5.8**	Der Hafen sollte ein Schulungsprogramm zur Cybersicherheit ausarbeiten, um die Cybersicherheitskompetenz von IT-Mitarbeitenden und Beschäftigten zu verbessern, die mit IT/OT-Assets arbeiten.
●●●	**[OPP] 5.9**	Alle Beschäftigten, die mit vernetzten maschinellen Anlagen arbeiten, sollten in den praktischen Grundlagen der IT/OT-Cyberhygiene fortgebildet werden.

Was versteht man unter einem „starken Passwort“?

Ein starkes Passwort ist ein Passwort, das von einem Menschen oder Computer nur schwer zu erraten ist. Aber Achtung: Manche Menschen programmieren Computer so, dass sie in einer Sekunde Tausende von Passwörtern ausprobieren. Was kann man also tun? Die meisten Systeme geben Komplexitätsregeln für Passwörter an (Mindestanzahl an Zeichen, Buchstaben, Zahlen, Sonderzeichen usw.). Das ist ein guter Ansatz, aber er reicht nicht aus, denn es ist möglich, auch unter Anwendung dieser Regeln ein schwaches Passwort zu erstellen, zum Beispiel „P@ssw0rd“. Zu den bewährten Verfahrensweisen gehört, dass ein Passwort ausreichend lang ist (mindestens 8, besser noch 10 Zeichen) und nicht auf einem Wörterbucheintrag basieren darf, auch nicht entfernt. Es darf ebenfalls nicht mit einer bestimmten Tastenanordnung in Verbindung stehen („qwerty“, „azerty“, „123456“ usw.) oder einen Zusammenhang mit dem Nutzer aufweisen (Geburtsdatum, Vorname eines Kindes usw.). Aktuell tendiert man bei den bewährten Verfahrensweisen dazu, den Einsatz der sogenannten „Multi-Faktor-Authentifizierung“ auszubauen, bei der das Passwort durch ein weiteres Authentifizierungsmittel (z. B. einen per SMS, E-Mail oder auf eine Smartphone-Anwendung verschickten Einmalcode) ergänzt wird. Die in Regel [OPP] 5.2 angesprochenen Leitlinien im Umgang mit Passwörtern sollten die in dieser Hinsicht zu befolgenden Regeln und Empfehlungen im Einzelnen aufführen.

Fallstudie
Sensibilisierungsprogramme für Beschäftigte

Dieser Leitfaden betont, dass allen Beschäftigten, Lieferanten und anderen Beteiligten eine Aufgabe bei der Gewährleistung der Cybersicherheit des Hafens zukommt. Wie im Zusammenhang mit den in Teil 1 dieses Leitfadens beschriebenen Angriffsszenarien beschrieben, ist ein erheblicher Anteil an Cybersicherheitsvorfällen auf menschliche Fehler zurückzuführen. Deshalb kommt der Umsetzung eines Sensibilisierungsprogramms für die Beschäftigten unter den Risikominderungsmaßnahmen eine zentrale Bedeutung zu; sie ermöglicht dem Hafen einen „raschen Erfolg“, wenn eine Steigerung der Cybersicherheitsreife erreicht werden soll. Zur Erleichterung dieser Aufgabe bietet diese Fallstudie eine Übersicht über die zur Einführung eines Sensibilisierungsprogramms für Cybersicherheit erforderlichen Schritte, beschreibt die Arten von Modulen, die in diese Programme aufgenommen werden können, und liefert einige wichtige Erfolgsfaktoren für ihre Durchführung.

Übersicht über die Schritte

Schritt 1

Ermitteln Sie einen Basisrichtwert, der den im Hafen herrschenden Bewusstseinsstand in Bezug auf Cybersicherheit wiedergibt. Eine solche Beurteilung der aktuellen Reifeniveaus innerhalb des Hafens wird dem Management dabei helfen zu erkennen, wo das Sensibilisierungsprogramm ansetzen sollte, und besondere Schwerpunkte zu ermitteln, auf die das Programm eingehen sollte, sowie einen klaren Reifegrad zum Ergebnis haben, auf dessen Grundlage sich die Fortschritte im Laufe der Sensibilisierungsveranstaltungen mitverfolgen lassen. Dies könnte anhand eines an die Beschäftigten versandten Fragebogens oder einer anderen formlosen Erhebungsmethode erfolgen.

Schritt 2

Entwerfen Sie eine Strategie zur Sensibilisierung in Sachen Cybersicherheit für den Hafen. Eine solche Strategie sollte greifbare Ziele, einen realistischen Zeitplan, eine Verteilung der Rollen und Verantwortlichkeiten und ein entsprechendes Budget umfassen. Um die Wirksamkeit der Programmeinführung zu gewährleisten, sollte bei der Vorstellung dieser Strategie die Zustimmung der Direktion eingeholt werden.

Schritt 3

Wählen Sie das Format für die durchzuführenden Sensibilisierungsmodule. Eine Sensibilisierungskampagne kann von einem Pflichtkurs über Webinare und Trainingsübungen bis hin zu Phishing-Übungen reichen. Die einzelnen Sensibilisierungsmodule sollten so ausgewählt werden, dass sie den in der Strategie festgelegten Kriterien entsprechen, insbesondere hinsichtlich des zeitlichen Rahmens und Budgets, die dem Hafen zur Verfügung stehen. Sensibilisierungsprogramme können auch in Zusammenarbeit mit externen Experten entwickelt werden, wenn die Organisation selbst nicht über das Know-how für die Gestaltung einer solchen Initiative verfügt. Diese Programme können auch für den privaten IT-Gebrauch von Beschäftigten bei sich zu Hause relevant sein.

Schritt 4

Führen Sie das Sensibilisierungsprogramm durch.

Schritt 5

Dokumentieren Sie die Ergebnisse. Zur Erfüllung rechtlicher Anforderungen bzw. für die Bedürfnisse des Hafens im Hinblick auf seine Entwicklung sollte nach Abschluss des Sensibilisierungsprogramms das Feedback der teilnehmenden Personen eingeholt werden. Die durch das Programm angestrebten und erreichten Sensibilisierungsziele sollten in einer Übersicht dokumentiert und gespeichert werden. Außerdem sollten die Organisationen auf eine fortlaufende Verbesserung achten, indem sie gute Ergebnisse und Verbesserungsmöglichkeiten für das Sensibilisierungsprogramm festhalten.

Schritt 6

Planen Sie die nächste Wiederholung. Um wirksam zu bleiben, sollten Sensibilisierungsprogramme aktualisiert und erneut durchgeführt werden, um mit den Entwicklungen im Hafen Schritt zu halten. In Abstimmung mit der Direktion sollte für die zweite Phase ein festgelegtes zeitliches Ziel angestrebt werden.

Typen von Sensibilisierungsmodulen für die Cybersicherheit

Sensibilisierungsprogramme und -initiativen können vielerlei Formen annehmen und entsprechend den Bedürfnissen des Hafens angepasst werden. In der nachfolgenden Tabelle finden Sie eine Beschreibung der wichtigsten Typen von Sensibilisierungsmodulen.

Typ Sensibilisierungs-modul	Kurzbeschreibung	Hauptvorteil(e)	Hauptnachteil(e)
Präsenz- oder Online-Kurs	Sensibilisierungs kurse werden als Echtzeit-veranstaltung mit einer Lehrkraft in Kursformat angeboten.	• Eigene Lehrkraft, die das Verständnis sicherstellt und auf Fragen antwortet • Anwesenheit und Aufnahme des Kursmaterials können überprüft werden.	• Zeit- und ressourcenintensiv, Einsatz während der Arbeitszeit erforderlich. • Kostenintensive Lösung.
E-Learning	Das Kursangebot wird automatisch über eine Online-Plattform zur Verfügung gestellt, normalerweise in Form von Videos.	• Heutzutage gibt es ein großflächiges Angebot an Online-Sensibilisierungskursen, einige davon sogar kostenlos • Kurse können von den Beteiligten online absolviert werden.	• Schwierigkeit, Anwesenheit und Aufnahme des Kursmaterials zu überprüfen.
Serious Games	Beteiligte „spielen“ ein Online- oder Handyspiel, das darauf ausgelegt ist, das Bewusstsein für Cybersicherheit zu schärfen, und werden dann in einer Nachbesprechung auf die wichtigsten Erkenntnisse und Erfahrungen aufmerksam gemacht.	• Spielerische und ungewohnte Formen der Vermittlung von Information können die Aufmerksamkeit fesseln und das Erlernte nachhaltig im Gedächtnis verankern • Die Verbreitung dieser Form des Trainings erfordert weniger Engagement seitens der Teilnehmenden.	• Es erfordert detaillierte Planung, ein passendes Serious Game auszuwählen, es entsprechend den Bedürfnissen der Organisation zu konfigurieren und das Sensibilisierungsprogramm durchzuführen. • Schwierigkeit, die Aufmerksamkeit für das Spiel bis zum Abschluss sicherzustellen.
Phishing-Übungen	Simulationsübung, in der eine Phishing-Mail an das Hafenpersonal geschickt wird. Wer auf das Phishing hereinfällt, wird identifiziert und in der Regel auf ein Sensibilisierungs-modul weiterverwiesen.	• Konkrete und unvergessliche Erfahrung für alle, die diesen Test nicht bestehen. • Die Arten von Beteiligten, die auf die Phishing-Aktion hereinfallen, können dokumentiert und statistisch erfasst werden.	• Behandelt nur eine Form der Bedrohung, das Phishing. • Trägt nicht zur Steigerung des Risikobewusstseins derjenigen bei, die den Test bestehen, und schließt nicht aus, dass ein „Bestehen” darauf zurückzuführen ist, dass die E-Mail übersehen wurde.
Simulation einer Schad-programm-kampagne	Maßgeschneiderte Sensibilisierungskampagnen für Schadsoftware zur Ermittlung des Bewusstseins für Risiken durch externe Geräte und Verbindungen bei den Beschäftigten. Die Kampagnen sind wie die Phishing-Kampagnen aufgebaut, verbreiten aber Schadware. Schadware-Skripte sind nicht persistent, sie ermitteln nur die Echtzeitdaten des Opfers oder Systems.	• Konkrete und unvergessliche Erfahrung für alle, die daran teilnehmen. • Wirkt wie eine „Feueralarm-Übung”, indem eine Krise simuliert wird, die dazu beitragen kann, das Verhalten einer Organisation bei einer echten Krise zu verbessern.	• Die Planung und Durchführung dieser Simulation ist zeit- und arbeitsintensiv. Sie kann eine Unterstützung durch externe Dienstleister erfordern. • Bei Personen, die diesem Test unterzogen wurden und die Falle nicht erkannt haben, kann es zu einem Vertrauensproblem kommen.
Lehrmaterial	Monatliche neue Inhalte mit Erfahrungsberichten zu Beispielen für echte Angriffe in Organisationen, die dabei aufgetretenen Sicherheitsprobleme, die Auswirkungen dieser Angriffe, die angewandten Lösungen und die gewonnenen Erfahrungen; kann auch aktuelle Sicherheitsthemen von Interesse für das Gewerbe enthalten.	• Gestaltung und Verbreitung relativ leicht: Eine einfache E-Mail reicht aus. • Regelmäßige Massen-E-Mails mit Informationen halten die Beteiligten auf dem Laufenden.	• Schwierigkeit, den Wirkungsgrad zu überprüfen: Manche Beteiligte könnten die Kommunikation einfach ignorieren oder übergehen.
Events	Spezifische Veranstaltungen (Arbeitsfrühstück, Weiterbildungen in der Mittagspause usw.) als Gelegenheit für Diskussionen oder Demos zu einem Thema der Cybersicherheit.	• Bringt die Akteure der Organisation in einer Veranstaltung zusammen und ermöglicht den Austausch von Informationen. • Relativ einfache Gestaltung und Durchführung.	• Kurzlebige Interaktion. • Größere Schwierigkeit, den Zuwachs an Erkenntnissen und Risikobewusstsein aus einer einzelnen Veranstaltung zu evaluieren.

Haupterfolgsfaktoren eines Sensibilisierungsprogramms

1. **Abstimmung des Sensibilisierungsprogramms auf betriebliche Themen und Herausforderungen**
   Wird ein Sensibilisierungsprogramm auf die betrieblichen Aspekte zugeschnitten, mit denen der Binnenhafen und seine Akteure konfrontiert sind, hat es eine größere Wirkung und ist somit erfolgreicher. Sensibilisierungsprogramme im Zusammenhang mit Binnenhäfen sollten sich spezifisch auf deren kritische Systeme und auf die möglichen Auswirkungen von Cyberangriffen auf Binnenhäfen konzentrieren.
2. **Beteiligung einer größtmöglichen Anzahl an Akteuren**
   Die Einbeziehung einer größtmöglichen Anzahl von Binnenhafen-Akteuren, einschließlich Drittbeteiligter und Lieferanten, sorgt dafür, dass sich die Verbesserung des Kenntnisstands und des Bewusstseins auf die gesamte Lieferkette auswirkt. Dieses Konzept ist für Binnenhäfen von besonderer Bedeutung, da eine erhebliche Anzahl von Drittbeteiligten im Alltagsbetrieb mitwirken.
3. **Messung von Wirkung und Fortschritt**
   Die beste Weise, die Wirksamkeit einer Sensibilisierungskampagne zu bewerten, besteht in einer Art von Wissenstest oder Evaluierung am Ende des Moduls. Dazu kann unter den Teilnehmenden eine kurze Befragung durchgeführt oder auch ein Quiz ausgeteilt werden.

Koblenz, Deutschland - Rhein

Fallstudie
Ausarbeitung einer Risikobewertung für Cybersicherheit

Für die Umsetzung der weiter oben beschriebenen Risikominderungsmaßnahmen, wie die Durchführung einer Cybersicherheitsstrategie, müssen die schützenswerten Assets ermittelt werden. Dazu werden die Häfen und ihre Akteure an einem gewissen Punkt eine Cybersicherheits-Risikobewertung durchführen müssen. Aus einer solchen Übung ergeben sich die Bausteine für eine solide Cybersicherheitsstrategie. Tatsächlich geben die aktuellen bewährten Verfahrensweisen bedarfsorientierten Ansätzen, dem Verständnis der Prozesse und der Ermittlung kritischer Assets den Vorzug gegenüber den Ansätzen der Vergangenheit, die auf der Einhaltung von Vorschriften basierten. Die nachfolgende Fallstudie beschreibt die generischen Schritte einer gründlichen Bewertung der Cybersicherheitsrisiken für einen Hafen und unterstreicht einige der wichtigsten Erfolgsfaktoren, die sich bei der Bewertung ergaben.

Übersicht über die Schritte

Schritt 1

Ermittlung der Assets des Hafens und möglicher Auswirkungen eines Cybersicherheitsvorfalls auf diese Assets.

- Ermitteln Sie die wichtigsten Betriebsabläufe im Hafen sowie die Assets, die für ihre Ausführung erforderlich sind. Stellen Sie sicher, dass eine Reihe von Assets wie Kontrollsysteme, die Systeme des technischen Gebäudemanagements, Kontrollzentralen, CCTV/Alarmgeber, mit den Schiffen kommunizierende Navigationssysteme, Kabeltrassen, für Ladungsplanung und Frachtabfertigung verwendete Hafensysteme und die von einem Hafen gesammelten und gespeicherten Daten dabei Berücksichtigung finden.
- Legen Sie ein Kriterium für die den Assets zugewiesene Kritikalität fest: Welches sind die kritischsten Betriebsabläufe? Von welchen Assets ist ihre Durchführung abhängig? Befinden sich Assets darunter, die von mehreren Betriebsprozessen gemeinsam genutzt werden und deshalb für den Hafenbetrieb von zentraler Bedeutung sind?
- Dokumentieren Sie die Hafen-Supportsysteme. Notieren Sie, ob diese Systeme mit dem Internet verbunden sind oder ob sie von einer spezifischen Stromquelle abhängen.
- Ermitteln Sie auf der Grundlage einer Stichprobe dieser Assets die möglichen Auswirkungen auf die Geschäftstätigkeit im Falle einer Beeinträchtigung der Integrität oder Verfügbarkeit dieser Assets.
- **Wichtigstes Endprodukt :** eine Liste aller Assets und Geräte der Häfen. Geben Sie zu jedem Eintrag eine schwerwiegendere Konsequenz für die Geschäftstätigkeit an, falls das Asset oder Gerät in seiner Funktionsweise beeinträchtigt würde. Das Resultat sollte selbstverständlich geschützt sein und aufgrund seiner sensiblen Natur streng vertraulich bleiben.

Schritt 2

Beschreibung der Geschäftsprozesse des Hafens

- Erstellen Sie eine Abbildung der Geschäftsprozesse und der Assets, die für ihren Ablauf erforderlich sind.
- Dokumentieren Sie die Informationsflüsse und Datenaustausche, die die Voraussetzung für die Durchführung dieser Prozesse bilden. Daraus ergibt sich eine Übersicht über die Arten von Interaktionen von wesentlicher Bedeutung für die Betriebstätigkeit, deren Unterbrechung ernsthafte Folgen für die Geschäftstätigkeit haben könnte.
- **Wichtigstes Endprodukt**: ein Diagramm mit Daten- und Informationsströmen zu den drei Hauptleistungen, die vom Hafen angeboten werden. Dieses Endprodukt sollte ebenfalls geschützt sein und streng vertraulich bleiben.

Schritt 3

Ermittlung von Sicherheitsbedrohungen

- Ermitteln Sie mögliche Bedrohungen für die in Schritt 1 ermittelten Assets. Eine Sammlung von Bedrohungen kann anhand der bestehenden Forschungsarbeiten zu Bedrohungen der Cybersicherheit von Relevanz für das Hafenumfeld (wie weiter oben beschrieben) oder durch eine umfassendere Forschungstätigkeit zum Thema erstellt werden. Das ist nicht zwangsläufig eine sehr komplexe Aufgabe: Es ist möglich, eine Liste von Standard-Bedrohungen festzulegen und diese Risiken den Hafen-Assets zuzuordnen, um eine vollständige Liste einschlägiger Bedrohungen für einen Hafen zu erzeugen.
- **Wichtigstes Endprodukt :** ein Bericht mit Angaben zu den Hauptbedrohungen, denen der Hafen ausgesetzt ist.

Schritt 4

Bewertung der Durchführbarkeit und der Wahrscheinlichkeit der Umsetzung der Bedrohung

- Weisen Sie jeder Bedrohung eine Durchführbarkeitsbewertung zu. Diese Einschätzung kann anhand der Evaluierung verschiedener Parameter vorgenommen werden: das Vorhandensein von Vorkenntnissen über die Systeme, die das Risiko entstehen lassen können, die Notwendigkeit, für die Ausführung spezifischer Vorgänge über einen physischen Zugang oder ein bestimmtes Berechtigungsniveau zu verfügen, das Niveau an Benutzerinteraktion, das für die Erteilung von Berechtigungen vorliegen muss, die für die Operation vorausgesetzte technische Komplexität und die Fähigkeit des Hafens, diesen Bedrohungen durch resiliente Funktionsweisen (eventuell im Notbetrieb) zu begegnen.
- Weisen Sie jeder Bedrohung ein Angreiferprofil zu, um zu überprüfen, wie realistisch ihre Durchführung ist. Angreiferprofile können anhand der folgenden Bewertungen erzeugt werden: Über welches Kompetenzniveau muss der Angreifer für die Durchführung des Angriffs verfügen? Was ist seine Motivation/ Welcher Nutzen entsteht ihm aus der Umsetzung der Bedrohung? Wie viele Ressourcen und welche Kenntnisse/Informationen sind dafür erforderlich?
- Gleichen Sie das Angreiferprofil mit der Durchführbarkeits-information ab, um eine Wahrscheinlichkeitsskala für die Umsetzung der einzelnen Bedrohungen zu erhalten.
- **Wichtigstes Endprodukt**: eine Liste der größten Bedrohungen mit den Bewertungen der jeweiligen Durchführbarkeit und Eintrittswahrscheinlichkeit.

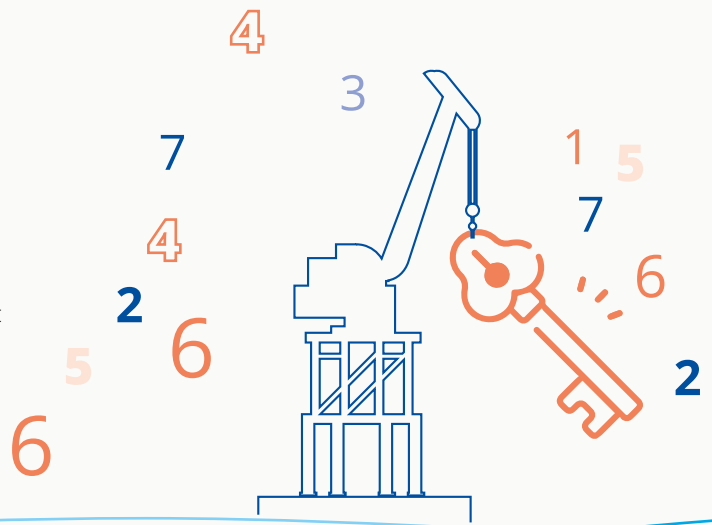
Schritt 5

Korrelierung der Wahrscheinlichkeit mit der Auswirkung der Bedrohung auf das Asset für die jeweiligen Bedrohungen

- Verwenden Sie eine Tabelle und stellen Sie eine Korrelation zwischen der möglichen Auswirkung eines Angriffs auf ein Asset des Hafens und der Wahrscheinlichkeit des Eintretens eines solchen Angriffs her. So lassen sich kritische Risiken (Risiken mit starker Auswirkung und hoher Wahrscheinlichkeit) jeweils gesondert betrachten.
- Damit haben Sie die Risikobewertung abgeschlossen, und die Direktion sollte jetzt über ein klares Bild der Hauptrisiken für die Cybersicherheit verfügen, mit denen der Hafen aktuell konfrontiert ist. Anhand dieser Risiken lässt sich eine Prioritätenliste für die Sicherheitsmaßnahmen erstellen oder eine vollständige organisatorische Cybersicherheitsstrategie erarbeiten.
- **Wichtigstes Endergebnis :** eine zweidimensionale Tabelle (Durchführbarkeit/Eintretenswahrscheinlichkeit), in der die Bedrohungen erscheinen und die in einem zweiten Schritt dazu beitragen kann, die erforderlichen Maßnahmen vorzusehen.

Wichtigste Erfolgsfaktoren für eine Cyberrisikobewertung

- **Bedeutung der Bedrohungen für die Hafentätigkeit**
  Die in der Bewertung untersuchten Bedrohungen sollten den Kontext des Hafentätigkeit berücksichtigen. Genauer gesagt bedeutet das, dass sich Häfen bei der Erstellung einer aussagekräftigen Bewertung von Bedrohungen auf diejenigen konzentrieren sollten, mit denen ihre Branche heutzutage konfrontiert ist, und dazu gegebenenfalls branchenspezifische Bedrohungsanalyse-Berichte hinzuziehen, Informationen mit Branchenkollegen (Peers) austauschen oder in Cybersicherheits-Arbeitsgruppen ihres Gewerbes mitarbeiten.
- **Ein unabhängiger und objektiver Blick auf mögliche Auswirkungen**
  Bei der Durchführung einer Selbstbeurteilung liegt die Herausforderung darin, das Bild zurückzustellen, das man sich von den eigenen Fähigkeiten und denen der eigenen Organisation macht, um zu einer objektiven Beurteilung der möglichen Auswirkungen eines Cyberangriffs zu gelangen. Dabei darf man keinesfalls vergessen, dass Folgenabschätzungen dazu da sind, auf begründete und faktische Art und Weise die potenziellen Auswirkungen eines Cybervorfalls auf ein Asset abzuleiten und keine Meinungsumfrage über eine vermutliche Auswirkung darstellen. Das Ergreifen von Maßnahmen zur Begrenzung nur vermuteter Auswirkungen könnte dazu führen, dass sehr aufwändige und kostspielige Arbeiten durchgeführt werden, die dennoch überflüssig sind, weil sie auf unbegründeten oder falsch angesetzten Hypothesen basieren.



Informationstechnologische (IT) / betriebstechnische (OT) Strategien für Häfen

Dieser Abschnitt, der auf Häfen und ihre Zulieferer ausgelegt ist, beschäftigt sich mit allgemeinen bewährten Verfahrensweisen für die Sicherheit von IT/OT-Systemen. Zur Erinnerung: Der Begriff IT/OT wird im Abschnitt „Einleitung“ dieses Leitfadens definiert. Vereinfacht gesagt, sind hier mit „IT“ Systeme gemeint, die sich mit der Verarbeitung von Daten befassen, während man unter „OT“ Systeme versteht, deren Ziel es ist, mit physischen Objekten zu interagieren. Beide Arten von Systemen können selbstverständlich auch untereinander interagieren, insbesondere dort, wo von „IT/OT-Systemen“ die Rede ist.

Dieser Abschnitt wendet sich an Hafenbeteiligte, die mit betrieblichen Systemen und Maschinen arbeiten, die in Binnenhäfen vorzufinden sind. IT/OT-Systeme können sich von einem Hafen zum anderen unterscheiden, werden aber allgemein als Systeme betrachtet, die betriebliche oder physische Aufgaben übernehmen, die über einen Computer oder ein angeschlossenes Gateway bedient werden. Im Hafenumfeld finden sich unter anderem:

- hafen-Verkehrsleitsysteme: Verkehrsüberwachungssysteme, Systeme für das Liegestellenmanagement, Instrumente zur Wetterüberwachung;
- navigationsgeräte, die mit Hafennetzwerken kommunizieren: AIS, GNSS;
- managementsysteme für den Terminalbetrieb: Betriebsanlagen, Umschlag- und Lagersysteme, Terminalbetriebssysteme;
- sicherheitssysteme: Zugangskontrolle, Anlagen zur Einbruchmeldung, Überwachungssysteme und andere Warnsysteme.

IT/OT-Systeme sind für die Cybersicherheit eines Hafens von besonderer Bedeutung, da sie künftig immer stärker vernetzt sein werden (insbesondere durch die wachsende Verbreitung von IoT-Geräten). Sie sind besonders anfällig, da sie oft ohne die in der heutigen IT-Software berücksichtigten Cybersicherheitskonfigurationen geplant wurden. Außerdem laufen sie häufig auf Altsystemen, die kaum oder gar keine Aktualisierungsmöglichkeiten vorsehen und häufig bei Cybersicherheitsprojekten und Wartungsplänen nicht mitberücksichtigt werden.

Allgemeine Verantwortungsstrukturen im Bereich IT/OT

Die Direktion oder ihre Vertretung sollte neben der im vorangegangenen Kapitel beschriebenen Festlegung von allgemeinen Rollen und Verantwortlichkeiten auch insbesondere die jeweiligen Verantwortungen für die IT/OT-Systeme zuweisen. Der Personenkreis, der mit diesen Systemen arbeitet, kann sich nämlich deutlich von der Gruppe der Personen unterscheiden, die mit dem Management des Betriebs und der IT-Systeme des Hafens betraut sind. Daher darf nicht vergessen werden, dass die Personen, die für den Hafenbetrieb kritische Anlagen und Systeme bedienen, eine wichtige Rolle bei der Gewährleistung der Cybersicherheit spielen. Diese betrieblichen Systeme sollten bei den Cybersicherheits-Risikoanalysen mitberücksichtigt werden.

	Nummer	Maßnahme
●●	[ITOT] 1.1	Es sollte ein Bestandsverzeichnis aller IT/OT-Assets geführt werden, die für den Betrieb des Hafens genutzt werden. Innerhalb dieses Bestandsverzeichnisses sollten die Assets nach der Kritikalität des Systems geordnet werden.
●●	[ITOT] 1.2	Die einzelnen Verantwortlichkeiten für die Cybersicherheit sollten für alle Beteiligten, die mit den im obengenannten Bestandsverzeichnis aufgeführten Assets arbeiten, klar definiert und kommuniziert werden, und zwar unabhängig davon, welcher Aspekt betroffen ist (beispielsweise Entwicklung, Integration, Betrieb, Wartung).
●●●	**[ITOT] 1.3**	Vor der Implementierung eines neuen IoT-Geräts oder Systems sollte eine Cybersicherheits-Risikoanalyse durchgeführt werden.
●●●	**[ITOT] 1.4**	Die kritischsten IT/OT-Assets sollten einer Cybersicherheits-Risikoanalyse unterzogen werden.

Identitäts- und Zugangsmanagement (Identity and Access Management – IAM)

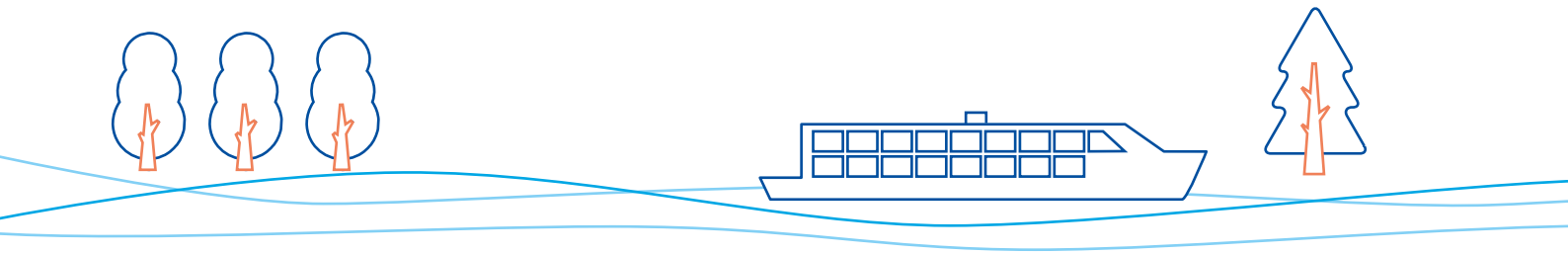
Häfen sollten eine klar definierte Politik für den Zugang zu und die Nutzung von Industriesystemen und vernetzten maschinellen oder anderen betrieblichen Anlagen für den Geschäftsbetrieb des Binnenhafens verfolgen. Für das Zugangs- und Identitäts-Management stehen die folgenden Maßnahmen zur Verfügung:

	Nummer	Maßnahme
●	[ITOT] 2.1	Der Zugang zu Maschinen und Systemen sollte möglichst nur über einen Benutzernamen und ein Passwort erfolgen können. Passwörter sollten sicher sein.
●	[ITOT] 2.2	Die voreingestellten Passwörter von betrieblichen Systemen sollten geändert und ein Verfahren zur regelmäßigen Passworterneuerung nach den von der Organisation festgelegten Leitlinien eingeführt werden.
●	[ITOT] 2.3	Dort, wo keine Authentifizierung möglich ist (insbesondere aufgrund betrieblicher Sachzwänge) sollten zusätzliche Maßnahmen in Betracht gezogen werden, einschließlich physischer Zugangskontrollen, Beschränkung der im System verfügbaren Funktionalitäten, Einführung einer Authentifizierung mittels Badges usw.
●●	[ITOT] 2.4	Häfen sollten dokumentieren, welche Beteiligten Zugang zu welchem kritischen System haben. Diese Liste sollte häufig aktualisiert werden.
●●	[ITOT] 2.5	Im Fall des Fehlschlagens einer Authentifizierung sollte einer Zeitverzögerung gegenüber einer Sperrung der Vorzug gegeben werden.
●●	[ITOT] 2.6	Für besonders sensible Systeme sollte die starke Multi-Faktor-Authentifizierung (beispielsweise mit PIN-Code und Smartcard) verwendet werden.

Physische Sicherheit

Da häufig ein direkter Zugang zu betrieblichen Systemen, industriellen Systemen und anderen Anlagen besteht (im Gegensatz zu anderen Assets wie Daten, IT-Komponenten, Software, IT-Anwendungen usw.), sollten auf diese Systeme zugeschnittene und anwendbare physische Schutzmaßnahmen eingeführt und durchgesetzt werden. Insbesondere die im Folgenden beschriebenen physischen Sicherheitsmaßnahmen sind Beispiele für bewährte Verfahrensweisen für den physischen Schutz von Assets gegen Cybersicherheitsrisiken.

	Maßnahmen-ID	Maßnahme
●	[ITOT] 3.1	Zugangspunkte für industrielle Kontroll- und Steuerungssysteme (ICS) und andere betriebliche Geräte sollten Unbefugten nicht zugänglich sein. Dies gilt insbesondere für Häfen, in denen viele Fußgänger oder Touristen verkehren.
●	[ITOT] 3.2	Zentraleinheiten von Workstations, Geräte für industrielle Netzwerke und speicherprogrammierbare Steuerungen (SPS) sollten in verschlossenen Schränken oder Räumen untergebracht werden.
●	[ITOT] 3.3	Im Hafen untergebrachte IT- und OT-Systeme sollten nach bewährten Verfahren zu ihrem Schutz (Brandmeldeanlagen, Klimaanlagen usw.) und ihrer Sicherheit (Zugang, CCTV usw.) geschützt werden.

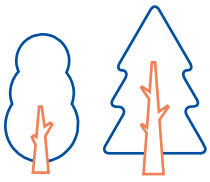


Wartung und Nutzung von IT/OT-Systemen

Wie weiter oben erwähnt, sind IT/OT-Systeme Cyberangriffen oft schutzlos ausgeliefert, weil sie auf veralteten Systemen laufen und damit von den üblichen Cybersicherheitsmaßnahmen wie System-Aktualisierungen und Patching ausgenommen sind. IT/OT-Systeme werden jedoch routinemäßig gewartet.

Eine bewährte Verfahrensweise bezüglich der Cybersicherheit besteht darin, einige grundlegende Sicherheitsmaßnahmen in die Wartungsprozesse von IT/OT-Systemen einzubeziehen. Auch bei der Außerbetriebnahme und der Entsorgung von IT/OT-Systemen sollte man die erforderlichen Sicherheitsaspekte berücksichtigen.

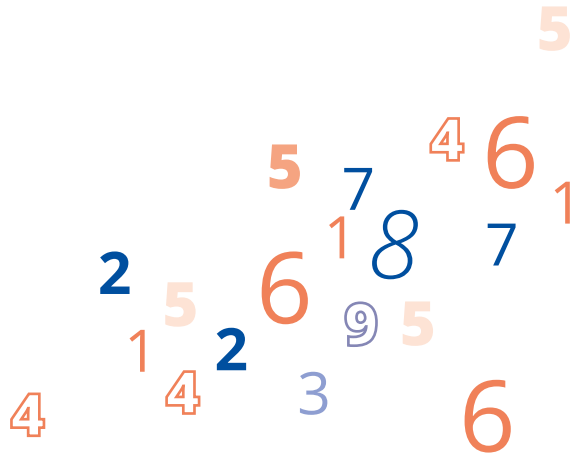
	Nummer	Maßnahme
●●	[ITOT] 4.1	Für die Aktualisierung der Wartung der betrieblichen Systeme sollte ein Verfahren festgelegt werden. Dieses sollte die Frequenz der Aktualisierung und die jeweilige Rolle und Verantwortung der Personen umfassen, die mit der Durchführung dieser Aktualisierungen beauftragt sind. Die System-Updates sollten, wenn anwendbar oder erforderlich, in mit den Anbietern abgeschlossenen Wartungsverträgen beschrieben werden.
●●	[ITOT] 4.2	Es sollten Instrumente oder Verfahren vorhanden sein, mit denen bei Aktualisierungsvorgängen des Systems die Unterschiede zwischen der aktuellen und der zu installierenden Version festgestellt werden können.
●●	[ITOT] 4.3	Alle Wartungsvorgänge sollten validiert werden. Es sollte ein Validierungsverfahren festgelegt und dem Personal mitgeteilt werden, die mit den betrieblichen Systemen arbeiten.
●●	[ITOT] 4.4	Für die Außerbetriebnahme betrieblicher Systeme sollte es ein Verfahren geben. Dieses sollte das Datum der Außerbetriebnahme, die am Vorgang beteiligten Parteien und die Einzelheiten der ordnungsgemäßen Entsorgung der Geräte dokumentieren.
●●●	**[ITOT] 4.5**	Bei Eingriffen und Aktualisierungsvorgängen sollte die Dokumentation folgende Punkte umfassen: • die Person, die die Arbeiten durchführt, sowie den Auftraggeber; • Datum und Zeitpunkt des Eingriffs; • Umfang der Arbeiten; • durchgeführte Tätigkeiten; • die Liste der ausgebauten oder ersetzten Geräte (einschließlich ihrer ID-Nummer, sofern vorhanden); • die vorgenommenen Veränderungen und deren Auswirkung.
●●●	**[ITOT] 4.6**	Es sollte ein Plan für regelmäßige Audits (deren Frequenz vom Hafen festzulegen ist) bestehen, anhand dessen sich die Einhaltung der Aktualisierungsverfahren beurteilen lässt. Im Anschluss an die Audits sollte ein Monitoring der Umsetzung der Empfehlungen aus dem Audit erfolgen.



Technische Sicherheitsmaßnahmen für IT/OT-Systeme

Die folgenden technischen Sicherheitsmaßnahmen sollten vom Hafenpersonal berücksichtigt werden, das mit der Konfiguration von Netzwerken, der Einrichtung und der Konfiguration von betrieblichen Systemen und der allgemeinen technischen Wartung dieser Systeme betraut ist. Allgemein gilt die Regel, dass kritische Systeme, wann immer möglich, sorgfältig von den allgemein zugänglichen Netzwerken und der übrigen IT-Infrastruktur abgeschottet werden sollen.

	Nummer	Maßnahme
●	[ITOT] 5.1	Für kritische Systeme (wie Schleusen- und Brückenmanagementsysteme, Kraftwerksanlagen, Trinkwasserversorgungsstationen) sollte der Zugang zum Internet auf ein Minimum beschränkt werden.
●	[ITOT] 5.2	Entwicklungstools sollten nicht auf aktiven oder laufenden Maschinen installiert werden. Auf IT/OT-Anlagen sollten nur MES-Systeme aktiv sein.
●	[ITOT] 5.3	Bei den betrieblichen Systemen sollten ungesicherte Protokolle (wie HTTP, Telnet, FTP) deaktiviert und durch gesicherte (wie HTTPS, SSH, SFTP) ersetzt werden.
●●	[ITOT] 5.4	Für die Verbindungen betrieblicher Systeme und sämtlicher IoT-Geräte, für das zu beruflichen Zwecken genutzte und für das öffentliche Wi-Fi sollten jeweils voneinander getrennte Netzzonen verwendet werden.
●●	[ITOT] 5.5	Industrielle Kontroll- und Steuerungssysteme (ICS) sollten in kohärente funktionale oder technische Zonen unterteilt werden. Diese sollten voneinander getrennt sein.
●●	[ITOT] 5.6	Es sollte eine Politik für das Filtern zwischen den Zonen und an administrativen Gateways eingeführt werden, die ein strenges, vorher festgelegtes Protokoll befolgt (d. h. Datenstromprotokollierung, Aktivitätsprotokollierung, IP-Adressprotokollierung usw.).
●●	[ITOT] 5.7	Wenn möglich, sollte an Gateways ein VPN eingerichtet werden, um den Datenverkehr mit der Außenwelt für betriebliche Systemzonen zu sperren.
●●	[ITOT] 5.8	Administratorenrechner mit umfangreichen administrativen Befugnissen sollten, wenn möglich, vom Hauptnetzwerk getrennt sein. Administratorenrechner sollten kontrolliert und für keine anderen Zwecke verwendet werden. Sie sollten häufig aktualisiert und durch Härtungsmaßnahmen verstärkt geschützt werden.
●●●	[ITOT] 5.9	Ist die Fernsteuerung eines betrieblichen Systems erforderlich, sollte die Fernverbindung zertifiziert sein, die Verbindungspasswörter sollten gemäß der durch die Organisation festgelegten Passwortstrategie verwaltet werden, die Protokollierung sollte aktiviert sein, sichere Kommunikationsprotokolle sollten vorhanden sein und die Fernverbindungen sollten automatisch beendet werden, wenn sie eine gewisse Zeit inaktiv waren.
●●●	[ITOT] 5.10	Es sollten Mechanismen vorhanden sein, die den Austausch von Maschine zu Maschine sichern (einschließlich EDI-Nachrichten und APIs, die hauptsächlich für die Kommunikation mit externen Partnern verwendet werden) und eine gegenseitige Authentifizierung, Integrität und Vertraulichkeit in Bezug auf die Hafensysteme gewährleisten, insbesondere, wenn der Austausch über das Internet stattfindet. Beispiele hierfür wären Verschlüsselung, PKI oder digitale Zertifikate, Integritätsprüfungen und Zeitstempel.



Überwachung von IT/OT-Systemen

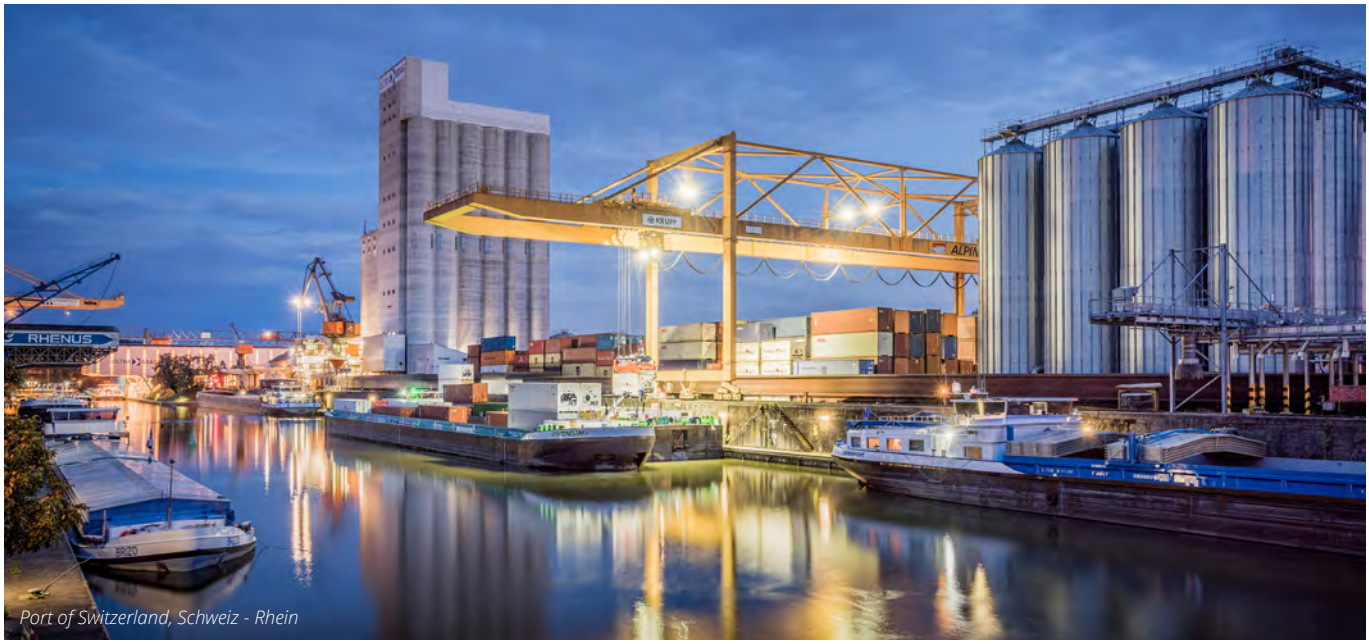
Häfen mit wenig betrieblichen Assets oder mit begrenzten Ressourcen können sich Überwachungsmaßnahmen für ihre betrieblichen Systeme unter Umständen nicht leisten. Die Direktion sollte solche Maßnahmen jedoch in Betracht ziehen, wenn die betrieblichen Systeme für die Hafentätigkeit eine kritische Bedeutung haben und wenn eine ihrer strategischen Prioritäten bei der Cybersicherheit darin besteht, Cyberbedrohungen für ihre Systeme aufzuspüren oder im Vorfeld zu erkennen.

	Nummer	Maßnahme
●●	[ITOT] 6.1	Veränderungen der Parameter von kritischen betrieblichen Systemen sollten nachverfolgt und protokolliert werden.
●●	[ITOT] 6.2	Auf kritischen betrieblichen Systemen sollten die Funktionen zur Nachverfolgung von Aktivitäten und Ereignissen aktiviert sein.
●●●	**[ITOT] 6.3**	Die Systemeigentümer sollten ein Verfahren für das Management der die betrieblichen Systeme betreffenden Cybersicherheitsvorfälle vorsehen. Dieser Prozess sollte die Speicherung von Ereignissen definieren (ob Protokolle gespeichert werden, wie sie gespeichert werden, wie sie gesichert und physisch geschützt sind), grundlegende Angaben dazu enthalten, wie eine anormale Systemaktivität definiert ist, und sollte die Bedingungen umfassen, ob und wann ein Ereignis als Cybersicherheitsvorfall zu melden ist.
●●●	**[ITOT] 6.4**	Für die Überwachung der Cybersicherheit der betrieblichen Systeme sollte der Hafen auch kommerzielle Überwachungsinstrumente in Erwägung ziehen.

Reaktion auf Cybervorfälle und Krisenmanagement für IT/OT-Systeme

Als Ergänzung zu den im Zusammenhang mit den organisatorischen Strategien und Verfahren erwähnten Maßnahmen zur Reaktion auf Vorfälle und zum Krisenmanagement sind die nachfolgenden Maßnahmen direkt für die Beteiligten vorgesehen, die mit IT/OT-Systemen arbeiten.

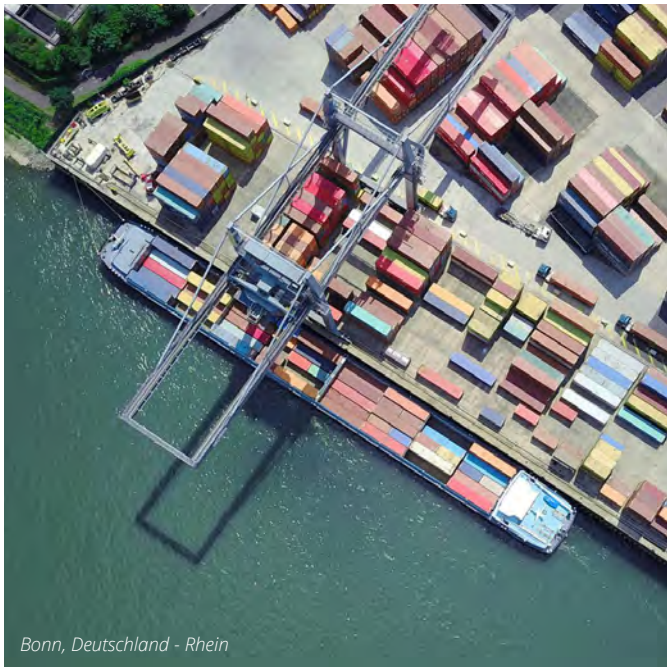
	Nummer	Maßnahme
●●	[ITOT] 7.1	Es sollte ein Cybervorfall-Managementplan definiert werden, der zur spezifischen Anwendung auf IT/OT-Systeme vorgesehen ist. Dieser Plan sollte die Einzelheiten zur Sicherung der für den Betrieb der IT/OT-Systeme erforderlichen Daten enthalten, die Eingriffsverfahren und die Verfahren zur Aktivierung des Notfallmodus der IT/OT-Systeme beschreiben sowie die Rückverfolgbarkeit der Maßnahmen vorsehen, die im Rahmen der Bewältigung eines Vorfalls ergriffen wurden.
●●	[ITOT] 7.2	Für die betrieblichen Systeme sollten Modi für den eingeschränkten Betrieb zur Verfügung stehen, die es bei einem Vorfall ermöglichen, den Betrieb anzuhalten oder manuell weiterzuarbeiten.



Port of Switzerland, Schweiz - Rhein

Sicherung von Navigationssystemen

Dieser Abschnitt wurde in den Text aufgenommen, um einige Risikominderungsmaßnahmen für die oft kritischen IT/OT-Navigationssysteme vorzustellen, die eine Verbindung zwischen dem Hafen und den navigierenden Schiffen darstellen. Im Rahmen dieses Leitfadens wurden nur Systeme von Relevanz für die Häfen berücksichtigt. Systeme von ausschließlicher Relevanz für die Besatzung oder das Schiff werden in diesem Leitfaden nicht behandelt. Die Minderungsmaßnahmen könnten es ermöglichen auf Risiken einzugehen, die im Rahmen der weiter oben beschriebenen spezifischen Angriffsszenarien für Häfen dargestellt wurden.



Bonn, Deutschland - Rhein

	Nummer	Maßnahme
●●	[ITOT] 8.1	Den Nutzern sollte ein Notfallhandbuch an die Hand gegeben werden, das die Möglichkeiten beschreibt, alle automatischen Programmierungen der Kommunikationsgeräte außer Kraft zu setzen. Außerdem sollte das Personal darüber informiert werden, welche entscheidende Rolle es beim Erkennen von erratischem, anormalem Verhalten solcher Systeme spielen kann.
●●	[ITOT] 8.2	Bei der Überwachung der Netzwerksicherheit sollten die Hafenbetreiber besondere Vorsicht walten lassen, wenn diese Netzwerke Zugriff auf das elektronische Kartenanzeigesystem ECDIS haben, und dafür sorgen, dass diese Netzwerke vor Internetzugriff von außen geschützt sind. Software-Aktualisierungen und Patches in Verbindung mit ECDIS-Systemen sollten systematisch installiert werden.
●●●	[ITOT] 8.3	Häfen, die GNSS- und GPS-Signale senden und empfangen, sollten Abwehrmaßnahmen gegen die Risiken des Spoofing von Signalen in Erwägung ziehen. Diese Maßnahmen könnten die Implementierung von Tools und Techniken umfassen, die dazu beitragen, Anomalien in eingehenden Signalen festzustellen, wie beispielsweise ein sogenanntes RAIM (Receiver Autonomous Integrity Monitoring), mit denen sich Satellitensignale auf Inkohärenzen überprüfen lassen.
●●●	[ITOT] 8.4	Häfen, die AIS-Daten von Schiffen empfangen, sollten Risikominderungsmaßnahmen in Betracht ziehen, die eine Überwachung dieser Daten in Bezug auf möglicherweise anormales Verhalten bieten. Solche Datenüberwachungsaktivitäten können dazu genutzt werden, um unerwartete Veränderungen von Schiffsrouten oder von statischen Informationen zu erkennen, die möglicherweise Anzeichen für eine böswillige Absicht sein könnten.

Fallstudie
Schutz von Containerterminals

Die in einigen Häfen vorhandenen Containerterminals benötigen für ihren Betrieb zahlreiche IT/OT-Ausrüstungsgegenstände, weshalb sie sich für eine besonders interessante Fallstudie zur Implementierung von Risikominderungsmaßnahmen bei der Cybersicherheit von IT/OT-Systemen anbieten. Da viele Häfen festgestellt haben, dass es sich bei den Terminals um kritische Infrastrukturen handelt, enthält dieser Leitfaden eine Fallstudie, die sich mit den wichtigsten Diensten und Assets eines Containerterminals und dementsprechenden eventuellen Cyberrisiken befasst.

Dienste und Assets von Containerterminals

Die Funktion von Containerterminals besteht darin, im Auftrag von Kunden des Hafens Container von Schiffen für den Straßen- oder Schienentransport (bzw. umgekehrt) zu verladen. Containerterminals sind für ihre Interaktionen mit den Kunden, Beförderern und für ihre internen Aktivitäten in der Regel auf ein **Terminalbetriebssystem** (TOS - Terminal Operating System) angewiesen. Dieses Betriebssystem bietet über die Verbindung zu anderen Geräten die folgenden Dienste an:

Kundenanforderungsmanagement
Die Kunden haben Zugang zu einer online zugänglichen **Anwendungsplattform**, die Informationen und einschlägige Spezifikationen zu den Containern enthält (Art der Ware, Gewicht, Größe, Containerhandling usw.), die sie befördern lassen möchten. Diese Plattform ist auf die im Terminalbetriebssystem gespeicherten Informationen angewiesen.

Instandhaltung der Container
Das Terminalbetriebssystem zentralisiert Informationen über Beschädigungen an Containern sowie den Zustand der eingegangenen und ausgelieferten Container und **versendet** im Schadensfall **Kostenschätzungen** für deren Reparatur oder Reinigung an die Kunden.

Containerumschlag
Dieser erfolgt auf der Grundlage der im Terminalbetriebssystem gespeicherten Informationen (Größe, Lage, Umschlagsanforderungen und Containertyp, aber auch verfügbare Einrichtungen für die Lagerung der Container). Dieses System kann Informationen an **Containerverladebrücken/Krane** übermitteln, die daraufhin Container zur Lagerung oder Verlagerung heben, stapeln oder bewegen.

Operatives Personalmanagement
Das Terminalbetriebssystem sendet Informationen zu Aufgaben, Wartungsanforderungen oder anderen Elementen über **Tablets oder Handgeräte** an die Beschäftigten des Hafens.

Kundenfakturierung und Finanzverwaltung
Über das System werden **Rechnungen** über die erbrachten Leistungen direkt an die Kunden **verschickt**; Die Zahlungsbestätigungen gehen beim gleichen System ein und werden dort nachverfolgt.

Verwaltung von Drittparteien/Lieferanten
Am Containertransport beteiligte Drittparteien wie LKW-Fahrer haben Zugang zu einer Anwendung, mit der sie die Abholung oder Abgabe von Containern nachweisen können, und über die sie Informationen über die Abhol- und Anlieferungszeiten und -orte erhalten.

Cybersicherheitsrisiken für Betriebssysteme von Containerterminals

Im Zusammenhang mit diesen Assets und den oben beschriebenen Diensten konnten durch den Abgleich zwischen der Eintrittswahrscheinlichkeit und der potenziellen Auswirkung auf die Betriebssysteme von Containerterminals zwei bedeutende Cybersicherheitsrisiken ermittelt werden:

- Ein **Ransomware-Angriff** auf Containerterminalsysteme, insbesondere auf ein Terminalbetriebssystem, der die Geschäftsabläufe des Containerterminals einfriert. Ein solcher Angriff verhindert, dass die Arbeitsabläufe des Terminalbetriebssystems ordnungsgemäß vor sich gehen und hat damit Auswirkungen auf einige oder sämtliche oben genannten Dienste. Es soll darauf hingewiesen werden, dass bei Containerumschlagskranen, die nicht ohne die im Betriebssystem des Terminals gespeicherten Daten arbeiten können, der Umschlagbetrieb gestört würde oder gar zum Erliegen käme.
- Ein böswilliger Eindringling, dem es gelungen ist, **kritische Daten** über das Laden und Entladen von Containern, deren Standort oder über Einzelheiten zu ihrem Inhalt **abzufangen**, könnte illegale Handlungen begehen (Diebstahl, Schmuggel oder Entnahme illegaler Ware). Während es sich für einen Eindringling schwierig gestalten könnte, aufgrund der Größe und der erforderlichen Transportlogistik einen Container physisch zu stehlen, könnte er stattdessen das Hafensystem ausspionieren und sich Informationen über den Standort und die Bewegung eines bestimmten Containers verschaffen, wie im oben beschriebenen Szenario dargestellt. Dies könnte den Ruf des Hafens ernsthaft schädigen und seine Sicherheit beeinträchtigen, und darüber hinaus zur Folge haben, dass er für die Konsequenzen des Abfangens dieser Daten haftbar gemacht wird.

Technische Cybersicherheits-maßnahmen für Häfen

Die weiter unten genauer beschriebenen technischen Cybersicherheitsmaßnahmen richten sich an die IT- bzw. Informationssicherheitsabteilungen eines Hafens oder einer Organisation, die mit Häfen arbeitet. Auch wenn die im Folgenden empfohlenen Maßnahmen an das Hafenumfeld angepasst wurden, handelt es sich um allgemeine Maßnahmen der IT-Sicherheit, die sich in allen Organisationen mit einer soliden Informationssicherheitspolitik wiederfinden. Es muss darauf hingewiesen werden, dass sich nicht jede Maßnahme für Häfen mit begrenzten Ressourcen und Personal, wie Häfen ohne eigene IT-Abteilung, relevant oder umsetzbar ist. Trotzdem sollte man sich mit diesen Maßnahmen vertraut machen, da sie einen guten Ansatz dafür bieten können, welche grundlegenden Erwartungen an die Sicherheit zu berücksichtigen sind, wenn eine Organisation im IT-Bereich einen gewissen Reifegrad erreicht hat.

Identitäts- und Zugangsmanagement (IAM)

Mit diesem Abschnitt sollen Sicherheitsmaßnahmen vorgestellt werden, die sich auf das Nutzermanagement auf IT-Systemen und -Geräten des Hafens beziehen. Für die Zwecke dieses Leitfadens werden die auf allgemeine IT-Systeme anwendbaren IAM-Maßnahmen getrennt von den Sicherheitsmaßnahmen für Betriebstechnologien behandelt. Nähere Informationen zu spezifischen IAM-Maßnahmen für IT/OT-Systeme sind unter [ITOT] 4 beschrieben. Aus praktischen Gründen können jedoch beide Themen gemeinsam behandelt werden.

	Nummer	Maßnahme
●	[TSM] 1.1	Der IT-Sicherheitsbeauftragte sollte sicherstellen, dass die Authentifizierungsoptionen auf allen PCs oder Tablets sowie bei jeder Software oder Anwendung aktiviert sind und die Passwörter regelmäßig geändert werden. Für Passwörter sollten, sofern wie möglich, eine Komplexitätspolitik und Komplexitätsregeln bestehen.
●	[TSM] 1.2	Alle Nutzer der IT-Systeme sollten identifiziert werden und auf den eigenen Namen lautende Einzelkonten verwenden.
●	[TSM] 1.3	Drittparteien und Lieferanten sollte ein Zugang zu IT-Systemen oder Datenbanken des Hafens nur für einen spezifischen Zeitraum und Zweck gewährt werden.
●	[TSM] 1.4	Es sollte zwischen „Benutzer"-Konten und „Administrator"-Konten unterschieden werden. Ein „Administrator"-Konto sollte nur denjenigen zugeteilt werden, die es benötigen. „Benutzer"-Konto-Privilegien sollten auf das strikte Minimum reduziert bleiben. Berechtigungen sollten nach dem „Segregation-of-duties-Prinzip (Funktionstrennungsprinzip) erteilt werden, d. h. jeder Nutzer sollte nur auf die Daten zugreifen können, die er für die Ausführung seiner Aufgaben benötigt, und ausschließlich für diese Aufgaben.
●	[TSM] 1.5	„Administrator"-Konten sollten nur für administrative Vorgänge wie die Verwaltung von Benutzerkonten, die Installation oder Aktualisierung von Software oder Wartungszwecke verwendet werden. „Administrator"-Konten sollten nicht für andere Aktivitäten wie eine Websuche oder die Beantwortung von E-Mails benutzt werden.
●	[TSM] 1.6	Anonyme oder generische Konten sollten aus den IT-Systemen entfernt werden.
●●	[TSM] 1.7	Es sollte ein Verfahren zur Erteilung und zum Entzug von „Benutzer"-Konto-Privilegien eingerichtet werden.
●●	[TSM] 1.8	Es sollte ein Verfahren zur Verwaltung des Lebenszyklus eines „Benutzer"-Kontos einschließlich seiner Erstellung, Änderung, Aktualisierung, Datensicherung und Löschung eingerichtet werden. Dieses Verfahren sollte auch die Einzelheiten für das Hinzufügen oder Entfernen von Geräten des Nutzers umfassen.
●●	[TSM] 1.9	Regelmäßig sollte eine Überprüfung der Zugangsrechte von Konten durchgeführt werden. Im Anschluss an eine solche Überprüfung sollten erteilte Rechte, die nicht gebraucht werden, entzogen werden. Alte Benutzerkonten sollten möglichst gelöscht oder, wenn das nicht möglich ist, deaktiviert/archiviert werden.
●●●	[TSM] 1.10	Je nach Anzahl der am Betrieb des Hafens beteiligten Personen sollten die Beteiligten die Verwendung eines Tools zur Verwaltung der Konten und Zugangsberechtigungen zu den IT-Assets des Hafens in Betracht ziehen. Zu den einschlägigen Beteiligten zählen Hafenverwaltungen, Terminalbetreiber, Gebietskörperschaften, Drittparteien usw.
●●●	[TSM] 1.11	Für die kritischsten Anwendungen und Datenbanken des Hafens, insbesondere für Datenbanken mit personenbezogenen Daten, sensiblen Betriebsdaten wie detaillierten Informationen über Schiffe, gefährliche Güter und Ladungsinformationen, sollte eine Multifaktor-Authentifizierung (MFA) in Betracht gezogen und angewendet werden (siehe Maßnahme [ITOT] 2.6).
●●●	[TSM] 1.12	Ein Verfahren für die Verwaltung privilegierter Konten (Privileged Access Management - PAM) mit den entsprechenden Sicherheitsanforderungen an diese Konten und Regeln für das Management ihres Lebenszyklus sollte definiert werden. Dieser Prozess sollte im Hinblick auf die privilegierten Konten von Drittparteien besonders nachdrücklich durchgesetzt werden.

Systemsicherheit

Dieser Abschnitt beschreibt Maßnahmen, die bei IT-Systemen und Assets durchgeführt werden sollten, um ihre Gesamtsicherheit zu verbessern. Diese Aufgaben werden höchstwahrscheinlich einer IT- oder IT-Sicherheitsfachkraft anvertraut werden müssen, da sie spezifische Konfigurationen von IT-Assets erfordern.

	Nummer	Maßnahme
●	[TSM] 2.1	IT-Teams sollten sicherstellen, dass auf allen Systemen des Hafens einschließlich Desktop-Computern und Servern Anti-Schadsoftware-, Antispam- und Antivirus-Software installiert ist und jeweils aktualisiert wird. Bei diesen Aktualisierungen sollte den sensibelsten und anfälligsten Komponenten der IT-Ausrüstung Priorität eingeräumt werden.
●●	[TSM] 2.2	Es sollte ein vollständiges Bestandsverzeichnis der IT-Asset geführt und regelmäßig aktualisiert werden, das Hardware, Geräte, Software, Systeme, Server, Netzwerke und Netzwerkkomponenten umfasst.
●●	[TSM] 2.3	Anhand des Asset-Bestandsverzeichnisses sollte eine entsprechende Aktualisierungspolitik definiert werden, die die Frequenz der Aktualisierung, die Mittel zu deren Durchführung, die Verantwortlichkeiten und mögliche Validierungsverfahren beinhaltet. Im Rahmen dieser Politik sollte spezifiziert werden, dass Aktualisierungen nur über vertrauenswürdige Quellen wie die offiziellen Websites von Herausgebern bezogen werden dürfen.
●●	[TSM] 2.4	Die IT-Teams sollten dafür sorgen, dass Remote-Verbindungen ordnungsgemäß gesichert sind, und dafür Techniken wie VPN mit hohen Verschlüsselungsniveaus verwenden. Benutzerpasswörter für den Zugriff auf Remote-Ressourcen müssen verstärkt oder mit zusätzlichen Sicherheitsvorkehrungen gekoppelt werden (Multifaktor-Authentifizierung, auf dem PC installiertes Zertifikat, Einmalpasswort usw.), damit sie keine Schwachstellen für Angriffe bieten. Es sollte geprüft werden, ob der Fernzugriff auf spezifische Nutzer oder Systeme beschränkt werden sollte.
●●	[TSM] 2.5	Es sollten Grundprinzipen zur Verwendung von Wechseldatenträgern (vorzugsweise deren Verbot) einschließlich USB-Sticks, CD-ROMs, externe Festplatten, Disketten usw. eingeführt werden.
●●●	[TSM] 2.6	Im Zusammenhang mit der Integration neuer Geräte in die Hafensysteme sollte ein Prozess für das Änderungsmanagement (im Sinne von ITIL) definiert werden.
●●●	[TSM] 2.7	Eine Liste des zulässigen Materials und der zulässigen Software (einschließlich der genauen Versionsangaben für jede autorisierte Software), sollte festgelegt und regelmäßig aktualisiert werden.
●●●	[TSM] 2.8	Die IT-Teams sollten eine Endpunkschutzstrategie für die Überwachung der Endgeräte im Hafen definieren (PC, Tablet, Telefon und alle mit dem Netz verbundenen Geräte, zu denen die Nutzer einen direkten Zugang haben), die dazu dient, diese Geräte zu überwachen und ihre Sicherheit durch die Implementierung von Sicherheitstools und -mechanismen wie Virenschutz, Verschlüsselung, Mobilgerätemanagement (Mobile Device Management - MDM) und Härtung (Erhöhung der Sicherheit durch Entfernen aller Anwendungen und Software, die standardmäßig installiert, aber für den beabsichtigten Zweck überflüssig ist) zu verstärken.
●●●	[TSM] 2.9	Die IT-Teams sollten Grundprinzipien und Regeln für die Installation und Konfiguration definieren und als Sicherheitsgrundsätze festlegen, so dass nur notwendige Dienste und Funktionalitäten installiert und nur für die Sicherheit sowie den Betrieb der Hafensysteme wesentliche Ausrüstungsgegenstände zugelassen werden.
●●●	[TSM] 2.10	Die IT-Teams sollten regelmäßige Audits der Software-Aktualisierungen und Server durchführen.

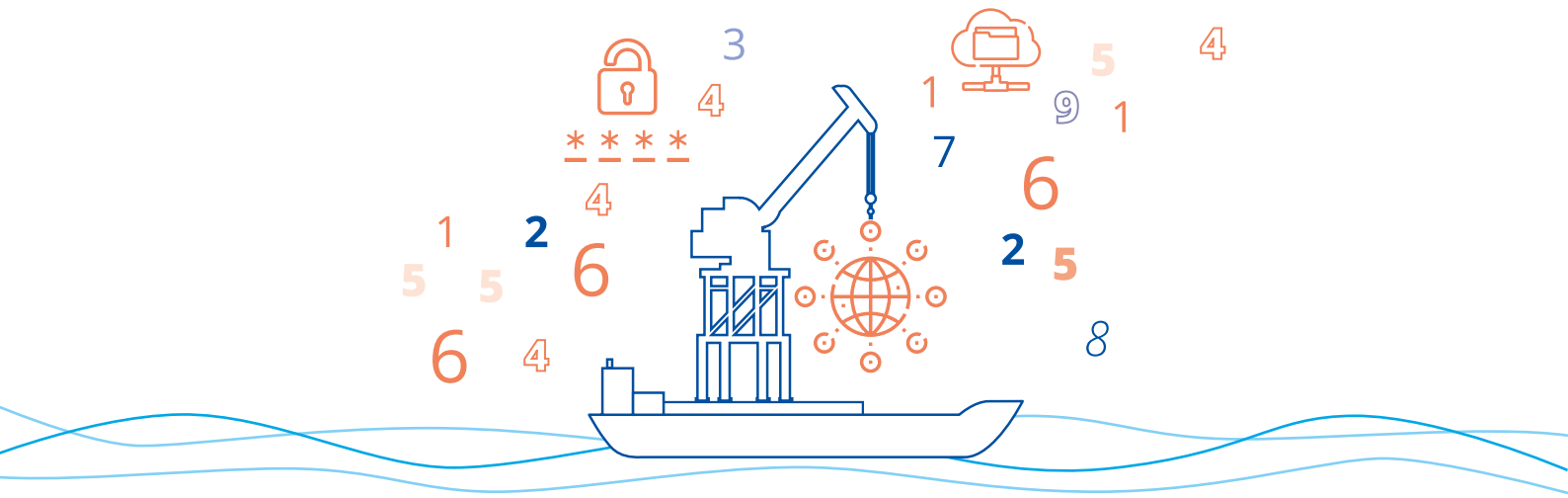
Netzwerksicherheit

Dieser Abschnitt beschreibt die Maßnahmen, die zum Schutz der von den Häfen genutzten Netzwerke ergriffen werden können. Wie beim vorangegangenen Abschnitt wird die Implementierung dieser Maßnahmen höchstwahrscheinlich die Beteiligung von IT-(Sicherheits)fachkräften erfordern. Falls ein Hafen nicht über eigenes IT-Personal verfügt, könnte die Heranziehung eines externen IT-Sicherheitsdienstleisters in Erwägung gezogen werden.

	Nummer	Maßnahme
●	[TSM] 3.1	Die IT-Teams sollten dafür sorgen, dass das Wi-Fi-Passwort komplex ist und regelmäßig geändert wird.
●	[TSM] 3.2	Die von den IT-Teams eines Hafens genutzten Wi-Fi-Netzwerke müssen so konfiguriert werden, dass sie das Verschlüsselungsprotokoll „WPA2 Enterprise“ oder „WPA3 Enterprise“ unterstützen. Ist das nicht möglich, sollte WPA3 (PSK)AES oder WPA3 (Personal oder Transitional) verwendet werden.
●●	[TSM] 3.3	Angemessene Regeln für die Netzwerkfilterung (beispielsweise im Hinblick auf IP-Adressen oder den autorisierten Datenverkehr) sollten eingeführt werden.
●●	[TSM] 3.4	Es sollte unterschieden werden zwischen professionellen Wi-Fi-Netzen (in der Regel für die berufliche Nutzung durch ordnungsgemäß authentifizierte Beschäftigte) und öffentlichen Wi-Fi-Netzen (in der Regel für Gäste/Besucher oder für die private Nutzung durch die Beschäftigten). Diese Netze sollten voneinander getrennt werden. Es sollten Grundprinzipien für die Netzwerktrennung angewandt werden, um die Verbreitung von Angriffen innerhalb der Hafensysteme zu verhindern und das Risiko eines Zugriffs über das Internet zu mindern.
●●	[TSM] 3.5	Netzzugangspunkte sollten durch die IT-Teams klar identifiziert und dokumentiert werden. Diese Liste sollte regelmäßig aktualisiert werden. Nicht benutzte Netzzugangspunkte sollten deaktiviert werden.
●●	[TSM] 3.6	Die IT-Teams sollten Grundprinzipien für autorisierte Geräte und Software festlegen und umsetzen, um sicherzustellen, dass nur vertrauenswürdige Komponenten in das Netzwerk des Hafens integriert werden.
●●●	[TSM] 3.7	Die Netzwerkregeln sollten regelmäßig überprüft und bei Bedarf angepasst werden. Außerdem sollten regelmäßig Netzwerkscans durchgeführt werden, um nicht autorisierte Netzwerkaktivitäten aufzuspüren.
●●●	[TSM] 3.8	Es sollten Grundprinzipien für die Meldung und Behandlung von anormalen Netzwerkaktivitäten festgelegt werden; dies sollte mit den in Maßnahme [OPP] 4.3. beschriebenen Verfahren zum Krisenmanagement koordiniert werden.
●●●	[TSM] 3.9	Es sollte eine Strategie für die Überwachung der Netzwerkaktivität festgelegt werden. Diese Strategie kann eine Reihe von Tools und Technologien zur Überwachung des Netzwerks umfassen. Sie sollte jedoch auch dafür sorgen, dass diese Tools durch fachlich ausgebildetes und kompetentes Personal genutzt, parametriert und regelmäßig geprüft werden.

Datenschutz

Dieser Abschnitt beschäftigt sich mit der Verwaltung der von den Hafenbeteiligten gesammelten, verarbeiteten und verwendeten Daten. Es wird darauf hingewiesen, dass Häfen in der Europäischen Union der Datenschutzgrundverordnung (DSGVO) aus dem Jahr 2016 unterliegen. Wenn die DSGVO auf Ihre Organisation anwendbar ist, muss diese im Hinblick auf den ordnungsgemäßen Umgang mit Daten und Informationen vorrangig konsultiert werden.



	Nummer	Maßnahme
●	[TSM] 4.1	Das betroffene Hafenpersonal sollte die auf sie anwendbaren gesetzlichen Vorschriften (wie die GSTVO) für die Sammlung und Haltung von Daten kennen. Es sollte eine Datenverwaltungsstrategie umgesetzt werden, die mit diesen gesetzlichen Vorschriften übereinstimmt und eventuell durch genauere Angaben oder Zusatzbestimmungen ergänzt wurde.
●●	[TSM] 4.2	Es sollte eine Datenhaltungsstrategie mit klaren Angaben zu den Regeln für die Datenklassifizierung und Datenvernichtung festgelegt werden. Personenbezogene Daten und andere besonders sensible Daten sollten für die Speicherung an dem Ort, an dem sie gespeichert sind, verschlüsselt oder gesichert werden, die gilt ebenfalls für den Datenverkehr im internen Netzwerk.
●●	[TSM] 4.3	Es sollte eine Strategie zur Datensicherung festgelegt und umgesetzt werden. Diese Daten-Backups sollten regelmäßig auf ihr Funktionieren getestet werden, wobei die Backups kritischer Systeme und Daten prioritär zu behandeln sind.
●●	[TSM] 4.4	Ein Plan zur Datenwiederherstellung (Data Recovery Plan - DRP) sollte erarbeitet werden, der das Protokoll beschreibt, das bei einem Cybersicherheitsvorfall oder einem anderen Vorfall zu befolgen ist, der zu Datenverlusten führen kann.
●●●	[TSM] 4.5	Es sollte eine Analyse der Datenbestände (data assets) abgefasst werden, die Informationen zu den folgenden Punkten enthält: • die Art von Daten, auf die der Hafen einen Zugriff benötigt, um den Mindestbetrieb (minimum required operations) aufrechtzuerhalten; • die Quellen der vom Hafen verarbeiteten Daten und Datenströme; • die Einzelheiten zur Speicherung der gesammelten und verarbeiteten Daten; • die aktuellen Zugangsrechte von internen Beteiligten und Drittparteien für die Datenbanken; • die Lebenszyklen der Daten und der Bedarf an Datenspeicherung und -haltung.
●●●	[TSM] 4.6	Mit Blick auf einen möglichen Cybersicherheitsvorfall müssen Reservefestplatten und Online-Datenspeicherplatz verfügbar sein.
●●●	[TSM] 4.7	Es sollten regelmäßig Untersuchungen der Netzwerkspeicher (NAS) durchgeführt werden, um potenzielle Störungen und Defekte an Datenspeichern, Daten oder Festplatten so früh wie möglich aufzudecken.

Schwachstellenmanagement und Systemüberwachung

Die Maßnahmen des Schwachstellenmanagements sollen dazu dienen, Informationen zu erhalten, mit denen bestehenden Schwachstellen besser behoben werden können. Diese Überwachungsaktivitäten können dazu beitragen, Schaden verursachende Aktivitäten innerhalb von Hafensystemen aufzudecken.

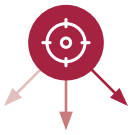
	Nummer	Maßnahme
●●	[TSM] 5.1	Häfen sollten ein Verfahren zur Cybersicherheitsüberwachung festlegen, das (den Mitarbeitenden, Anbietern, Dritten oder Branchenkollegen) die Möglichkeit bietet, auf neue Schwachstellen aufmerksam zu machen, damit rasch entsprechende Risikominderungsmaßnahmen ergriffen werden können. Dieses Verfahren sollte mit den die IT/OT-Systeme und deren Eigentümer betreffenden Verfahren koordiniert werden (s. [ITOT] 6.1).
●●	[TSM] 5.2	Die IT-Teams sollten einen Prozess für das Schwachstellenmanagement definieren, um (beispielsweise anhand von Schwachstellen-Scans) Schwachstellen bei den Assets zu identifizieren, sowie einen Prozess für den Umgang mit diesen Schwachstellen.
●●	[TSM] 5.3	Es sollte ein Protokollierungssystem zur Aufzeichnung von Aktivitäten und Ereignissen eingeführt werden, insbesondere von Ereignissen wie Benutzerauthentifizierung, Verwaltung von Konten und Zugangsrechten, Änderungen der Sicherheitsregeln sowie allen Änderungen oder Veränderungen der Funktionsweise der Hafensysteme.
●●	[TSM] 5.4	Für jede identifizierte Schwachstelle sollten entsprechende Risikominderungsmaßnahmen festgelegt und umgesetzt werden. Sofern das nicht möglich ist oder wenn keine Risikominderungsmaßnahmen festgelegt wurden, sollte eine entsprechende dokumentierte Erläuterung vorgehalten werden.
●●●	[TSM] 5.5	IT-Teams sollten Instrumente oder Verfahren zur Echtzeit-Überwachung der Verfügbarkeit von Hafensystemen und Geräten einrichten. Kritische Systeme (Administratoren-Rechner, Kommunikationsgeräte, Navigationsgeräte) sollten bei diesen Aktivitäten vorrangig behandelt werden.
●●●	[TSM] 5.6	Sofern es für notwendig erachtet wird und mit den vorhandenen Ressourcen und dem verfügbaren Personal umsetzbar ist, sollten Häfen Systeme zur Logdaten-Analyse und -Korrelation einführen, die dazu beitragen, Ereignisse zu identifizieren und Cybersicherheitsvorfälle aufzuspüren.

Teil 3

Tipps zur Umsetzung der Risikominderungsmaßnahmen

Dieser Teil soll die Umsetzung der oben beschriebenen Risikominderungsmaßnahmen erleichtern. Angesichts des breiten Spektrums und der verschiedenen Komplexitätsniveaus der vorgeschlagenen Maßnahmen sollten Häfen für deren Umsetzung Prioritäten festlegen, die ihren Ressourcen, dem angestrebten Reifegrad und ihren Cybersicherheitsbedürfnissen entsprechen.
Die untenstehende Tabelle enthält Vorschläge für Maßnahmen die auf der Grundlage von zwei Kriterien prioritär umzusetzen sind: dem Reifegrad des Hafens bezüglich seiner Cybersicherheit und den jeweils beteiligten Parteien.
Die Cybersicherheitsreife eines Hafens kann zu einem bestimmten Zeitpunkt gemessen werden, z. B. anhand des weiter unten vorgeschlagenen Bewertungsrahmens. Sobald der Reifegrad bekannt ist, kann dieser beibehalten, verstärkt oder erhöht werden. Jede dieser Optionen entspricht einem Aufwand und ist mit entsprechenden Kosten verbunden. Bei der Wahl des angestrebten Reifegrads muss die Direktion eine Vielzahl von Kriterien berücksichtigen, darunter die Größe des Hafens, seine Exposition, seine technologische Abhängigkeit, die Anzahl an Lieferanten und Unterauftragnehmern, seine technischen und finanziellen Mittel, aber auch seine Erfahrungen und seine eigene Cybersicherheitsproblematik.
Als Beispiele sind hier einige Kriterien aufgeführt, die bei der Bestimmung der angestrebten Cybersicherheitsreife helfen können. Diese Kriterien sind ausschließlich als Orientierung oder als Anregung für die Direktion gedacht und müssen von dieser selbst festgelegt werden.

Anzustrebender Reifegrad



Niedrig	Mittel	Hoch
Mögliche Kriterien • Der Binnenhafen ist kein bedeutender regionaler Knotenpunkt für Handel und Verkehr. • Die IT-Teams sind sehr klein oder bestehen nur aus externen IT-Fachkräften. • Für das Betreiben des Hafens wird fast keine digitale Infrastruktur benötigt.	**Mögliche Kriterien** • Der Hafen verfügt über einige größere Infrastrukturen, ist aber nicht der Mittelpunkt der regionalen Hafenaktivitäten. • IT-Dienstleister sind präsent und werden häufig tätig, bzw. innerhalb der Organisation gibt es eine Art von IT-Team. • Einige Aktivitäten des Hafens sind von der digitalen Infrastruktur abhängig.	**Mögliche Kriterien** • Der Binnenhafen gilt als wichtiger Knotenpunkt für den Handel in der Region. Er beherbergt eine große Transport-/Containerplattform oder verkörpert eine wichtige Transitzone. • Es gibt ein internes IT-Team und entsprechende Entscheidungsstrukture . • Der Betrieb des Hafens ist stark von der digitalen Infrastruktur abhängig und es ist sogar ein gewisses Maß an „SmartPort“-Technologien vorhanden.

Die verschiedenen berücksichtigten Beteiligten entsprechen den Akteuren, die jede der Maßnahmen umsetzen sollen. Eine Reihe der oben vorgeschlagenen Maßnahmen kann nur von IT- oder Sicherheitsfachkräften durchgeführt werden, während andere in die Zuständigkeit von Management oder der Direktion fallen.
Es liegt in der Natur der Sache, dass sich der Reifegrad nicht zu schnell ändern lässt. Ein Hafen, der seinen eigenen Reifegrad als „niedrig“ einstuft, kann nach einigen Jahren fortgesetzter Bemühungen einen „mittleren“ Reifegrad anstreben, aber nicht innerhalb der gleichen Frist direkt einen „hohen“ Reifegrad erreichen wollen, selbst wenn er darauf erhebliche finanzielle Mittel aufwendete. Denn Cybersicherheitsreife ist auch eine Frage der Erfahrung, der Kultur und der Praxis, und das braucht Zeit.
Der Reifegrad sollte zudem kohärent und so einheitlich wie möglich ausfallen. Beispielsweise sollte sich ein Hafen nicht mit einem „niedrigen“ Reifegrad für den Bereich „organisatorische Leitlinien und Verfahren“ zufriedengeben und gleichzeitig einen „mittleren“ oder „hohen“ Reifegrad für den Bereich „Netzwerksicherheit“ anstreben. Ebenso ist es sinnlos, sogar kontraproduktiv und ganz sicher kostspielig, eine Maßnahme umsetzen zu wollen, die zu einem «hohen“ Reifegrad zählt, solange nicht bereits eine überwiegende Mehrheit an Maßnahmen des „niedrigen“ und „mittleren“ Reifegrads durchgeführt wurden. Oft wird die Umsetzung von Cybersicherheitsmaßnahmen mit dem Bau von Befestigungsanlagen verglichen, und es liegt auf der Hand, dass es sinnlos ist, eine Flanke zu befestigen, wenn man die andere völlig ungeschützt lässt. Sehr oft treten Cybersicherheitsvorfälle dort auf, wo die Cybersicherheit die geringste Stärke aufweist. Deshalb muss eine gute Strategie darin bestehen, die schwächste Stelle zuerst zu stärken.

Es ist aber immerhin möglich, auch ohne die restlichen Aspekte zu vernachlässigen, in spezifischen Bereichen ein „Stückchen weiter“ zu gehen, wenn sich diese als besonders kritisch erwiesen haben.

Beurteilungsrahmen für den Reifegrad

Dieser Leitfaden möchte Ihnen hier einen Bewertungsrahmen anbieten, anhand dessen sie den jeweils aktuellen Reifegrad eines Hafens bestimmen können.

Es handelt sich hierbei um eine Methode zur Selbstbewertung, bei der für jede in Teil 2.

Im Idealfall sollte diese Selbstbewertung von einem kleinen multidisziplinären Team mit mindestens einer Vertretung aller Beteiligtengruppen durchgeführt werden, d. h.:

- ein Mitglied der Direktion, das idealerweise für die Cybersicherheit verantwortlich ist;
- ein Mitglied des IT-Teams, das einen guten Überblick über die Infrastruktur und die Anwendungen hat;
- ein Mitglied des operativen Managements, das über eine solide Kenntnis der Geschäftssysteme verfügt (bzw. mehrere Mitglieder, fall eine Person nicht ausreichen sollte, um alle Geschäftssysteme abzudecken).

Jedes Teammitglied sollte jede der Maßnahmen unabhängig von den anderen Mitgliedern bewerten. Idealerweise bewertet jedes Mitglied jede Maßnahme entsprechend seinem Wissen und seiner Sensibilität, bzw. zumindest alle Maßnahmen, die sich in seiner Spalte der Anwendbarkeitstabelle befinden, selbst wenn dazu bei einigen Punkten weitere Kollegen zu Rate gezogen werden müssen.

In einem zweiten Schritt setzen sich die Mitglieder zusammen und besprechen gemeinsam ihre Notizen. Dort, wo Abweichungen festgestellt werden, tauschen sie sich untereinander aus und erläutern die Gründe für ihre Bewertung. Nach diesem Austausch und unter Berücksichtigung der Bemerkung der anderen Mitglieder entscheidet das Mitglied, das den Beteiligten vertritt, dem die jeweilige Maßnahme zuzuordnen ist, über die Endnote.

Die Bewertungsskala umfasst die Noten von 1 bis 5 und kann wie folgt dargestellt werden:

Note	Beschreibung
1	Diese Maßnahme ist nicht koordiniert oder es ist kein Personal für ihre Durchführung vorgesehen. Es gibt kein formelles Programm oder spezifischen Kontrollen dieser Art.
2	Im Zusammenhang mit dieser Maßnahme gibt es zwar eine informelle Kommunikation oder auch einen informellen Prozess, jedoch keine Dokumentation und kein offizielles Verfahren.
3	Einige Rollen und Verantwortlichkeiten im Zusammenhang mit dieser Maßnahme sind formalisiert. Es gibt entsprechende Prozesse, die jedoch nicht systematisch auf ihre Umsetzung hin überprüft werden.
4	Die Rollen und Verantwortlichkeiten sind klar definiert, und es existieren formale Schritte zur Prozessüberprüfung, die sicherstellen, dass diese Maßnahme implementiert wurde.
5	Im Zusammenhang mit dieser Maßnahme gibt es eine „Kultur der ständigen Verbesserung“. Die ihr unterliegenden Prozesse werden im Hinblick auf ihr Verständnis und ihrer Verbesserung quantitativ überwacht.

Nach Abschluss dieses Selbstbewertungsprozesses wir der Notendurchschnitt für die Maßnahmen in jeder der drei Zeilen der untenstehenden Anwendbarkeitstabelle berechnet. Das Ergebnis besteht dementsprechend aus drei Durchschnittsnoten von 1 bis 5 für jeden Reifegrad (niedrig, mittel, hoch).

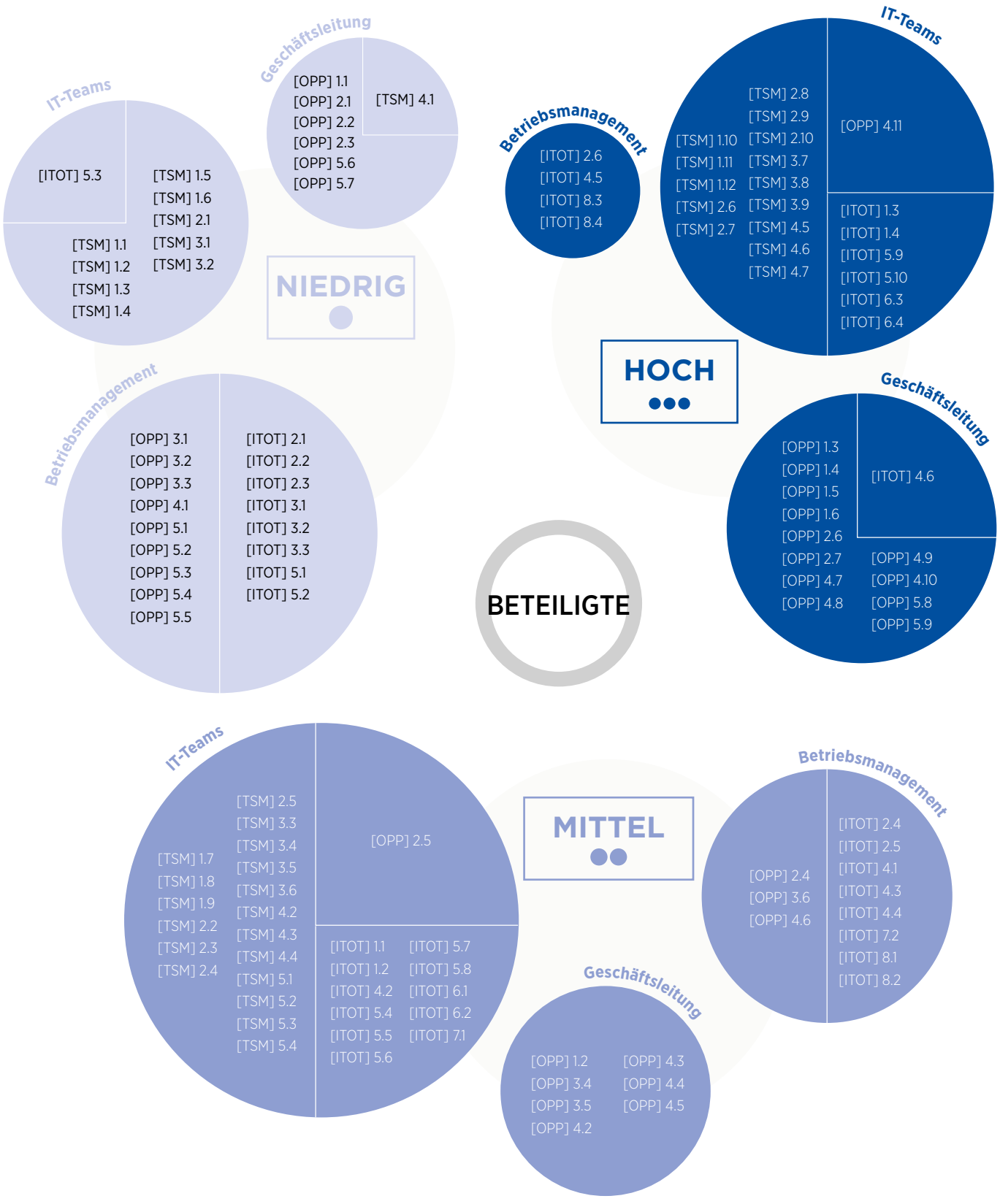
Der Reifegrad gilt als erreicht, wenn:

1. der Durchschnittswert der Maßnahmen des angestrebten Reifegrads mindestens 2,5 beträgt;
2. der Durchschnittswert der Maßnahmen des Reifegrads unmittelbar unter dem angestrebten mindestens 3,5 beträgt;
3. der Durchschnittswert der Maßnahmen des noch darunter liegenden Reifegrads 4 beträgt.

So muss für das Erreichen des Reifegrades „mittel“ der Durchschnittswert 2,5 oder darüber und der Durchschnittswert des Reifegrads „niedrig“ 3,5 oder darüber betragen. Um den höchsten Reifegrad zu erlangen, ist ein Durchschnittswert der Maßnahmen des mittleren Reifegrads von 3,5 oder darüber und beim niedrigen Reifegrad ein Durchschnittswert von 4 oder darüber erforderlich.

Tabelle zur Anwendbarkeit der Maßnahmen

Die untenstehende Tabelle beschreibt die Maßnahmen, die von den Beteiligten je nach dem von der Direktion angestrebten Reifegrad umgesetzt werden müssen:



Glossar

Düsseldorf, Deutschland - Rhein

Auswirkung

Dieser Begriff bezeichnet die Folgen eines Cybersicherheitsvorfalls bei dessen Eintritt (unabhängig von der Eintretenswahrscheinlichkeit). Die Schlüsselfrage in diesem Zusammenhang lautet also: Wenn ein bestimmter Cybersicherheitsvorfall eintritt, was passiert dann - schlimmstenfalls - als Nächstes? Von Anfang an kann es sich um größere oder geringere Auswirkungen handeln. Beispielsweise kann die Zerstörung eines Servers (der Cybersicherheitsvorfall) sehr unterschiedliche Auswirkungen haben, je nachdem, ob es sich um einen Server für Entwicklungszwecke oder um einen betriebskritischen Server handelt. Die Auswirkungen lassen sich jedoch verringern, indem man Umgehungsstrategien ausarbeitet und das System beispielsweise durch Notfallverfahren resilienter gestaltet. Im Falle des kritischen Servers könnte zum Beispiel ein zweiter Server bereitstehen, der die Aufgaben des ersten bei einem Ausfall übernimmt. Für den Fall eines Datenverlusts kann ein Backup vorgesehen sein usw. Die Auswirkungen werden immer ohne Berücksichtigung der Bedrohung (siehe Definition) bewertet.

Backdoor (Hintertür)

In einer Software bezeichnet man mit Backdoor eine dem rechtmäßigen Benutzer unbekannte Funktion, die einen geheimen Zugriff auf die Software ermöglicht.

Bedrohung

Unter Bedrohung versteht man einen Akteur, einen Umstand oder ein Ereignis, das eine negative Auswirkung auf eine Organisation (ihre Tätigkeit, ihre Assets, ihren Ruf oder auf mit ihr in Verbindung stehende Personen) hat bzw. über diese eine Auswirkung auf andere Organisationen, die mit ihr in Verbindung stehen, haben kann. Um eine solchen Auswirkung zu provozieren, muss die Bedrohung eine oder mehrere Schwachstellen gemäß einem bestimmten Szenario ausnutzen. Je plausibler das Szenario, desto größer ist die Verletzlichkeit, und je zahlreicher die Bedrohungen, desto größer die Eintretenswahrscheinlichkeit eines Cybersicherheitsvorfalls. In diesem Fall spricht man von einer hohen Bedrohungsstufe. So ist beispielsweise die Bedrohungsstufe eines im Internet exponierten Servers höher als die eines Servers, der nur innerhalb eines internen Netzwerks exponiert ist, da es potenziell mehr Personen gibt, die versuchen könnten, den Server zu hacken. Oft wird zur Verringerung der Bedrohung auf der Ebene der Schwachstellen angesetzt, entweder durch ihre Beseitigung (oder die Verringerung ihrer Anzahl), oder, indem man eine Ausnutzung komplexer macht (beispielsweise durch Hinzufügen von Schutzmechanismen). Bisweilen ist es möglich, direkt auf die Anzahl der Akteure, die Umstände oder Ereignisse Einfluss zu nehmen, die eine schädigende Wirkung haben könnten, Die Bewertung einer Bedrohung erfolgt immer ohne Berücksichtigung der Auswirkungen (siehe Definition).

BYOD

Diese Abkürzung steht für „Bring Your Own Device“ (Bringen Sie ihr eigenes Endgerät mit). Im Unternehmenskontext verweist dieser Begriff auf die Praxis von Mitarbeitenden, für ihre Arbeit eigene, persönliche Endgeräte zu verwenden, was vom Unternehmen entweder begrüßt oder Beschränkungen unterworfen wird. Meistens handelt es sich um Smartphones oder auch um Laptops. Die Beschäftigten schätzen den Komfort der Arbeit auf dem eigenen vertrauten Gerät. Für das Unternehmen kann eine solche Praxis Einsparungen mit sich bringen. Aus Sicht der Cybersicherheit können diese persönlichen Geräte eine Herausforderung darstellen, denn es ist oft unmöglich, diese hinreichend zu sichern, und die Vielfalt an Marken und Modellen steigern dieses Risiko noch.

CFM

„Cargo and Fleet Management“ (Ladungs- und Flottenmanagement)

Cybersicherheitsvorfall

Dieser allgemeine Begriff wird für ein Ereignis verwendet, das negative Folgen für die Cybersicherheit nach sich zieht. Die Ursache eines solchen Vorfalls kann auf einen Ausfall der Hardware zurückgehen (defekte Festplatte), einen Absturz (Neustart des Servers), Sabotage (bewusstes Einschleusen eines Computervirus), menschliches Versagen (versehentliches Klicken auf einen Link in einer Phishing-E-Mail) oder gar Fahrlässigkeit (ein Mitarbeitender schreibt seine PIN-Nummer auf die Rückseite seiner Smartcard). Wird rechtzeitig auf die Folgen eines solchen Vorfalls reagiert, gilt dieser Vorfall als abgeschlossen. Ist das nicht der Fall, kann aus dem Vorfall eine Cybersicherheitskrise werden, die sich ausbreitet und deren Folgen sich mehr oder weniger rasch über die Zeit verschärfen.

Hacktivismus

Computer-Hacking (beispielsweise durch Infiltration oder Störung eines Netzwerks oder einer Website) in der Absicht, die Ziele von politischem oder sozialem Aktivismus zu fördern.[10]

[10] https://www.merriam-webster.com/dictionary/hacktivism

Härtung (Hardening)

Prozess der Sicherung eines Systems durch das Entfernen von Komponenten, die für seinen Betrieb (z. B. bei einem PC oder Server) nicht erforderlich sind. Beim Härten wird die „Angriffsfläche" des Systems verringert, d. h. es werden alle standardmäßig installierten, aber überflüssigen Elemente entfernt, die (potenziell) Schwachstellen enthalten können (Anwendungen, Softwarebibliotheken, optionale Module usw.) Allgemein wird eingeräumt, dass die Anzahl an für einen Angriff nutzbaren Schwachstellen eines Systems mehr oder weniger proportional zur Anzahl seiner Codezeilen ist. Das Entfernen von nicht benötigten Komponenten bewirkt also auch, dass die Anzahl der von einem Angreifer nutzbaren Schwachstellen reduziert wird.

ITIL

Information Technology Infrastructure Library, eine Sammlung von Werken, die eine Referenz für bewährte Verfahrensweisen für das Management von Informationssystemen darstellen. ITIL hat weitgehend zur Einführung der Norm ISO/IEC 20000 beigetragen und wird in Unternehmen bisweilen einem Qualitätsprozess vergleichbar angewendet.

Kronjuwelen

Mit „Juwelen" werden Assets bezeichnet, die bei der Erfüllung der Aufgaben einer Organisation die kritischste Rolle spielen. Um zu bestimmen, um welche Assets aus der Gesamtheit aller Assets es sich handelt, ist eine Analyse erforderlich.[11]

LBM

Diese Abkürzung steht für „Lock and Bridge Management" (Schleusen- und Brückenmanagement). Das Management von Schleusen und Brücken erfolgt über Bauwerke wie bewegliche Brücken, Einrichtungen zur Veränderung des Wasserstands wie Staustufen und Schleusenanlagen, die besonders kritische Systeme darstellen, da sie bei einem Cyberangriff weitreichende Überschwemmungen verursachen können.

Phishing

Eine Form des Betrugs, bei der ein Internetnutzer (beispielsweise durch eine betrügerische E-Mail) dazu verleitet wird, personenbezogene oder vertrauliche Informationen preiszugeben, die der Betrüger zu unlauteren Zwecken verwenden kann[12].

Risiko

Dieser Begriff wird in der Cybersicherheit formal dazu verwendet, um eine Reihe von Bedrohungen zu bewerten, denen ein System mit mehr oder weniger großer Wahrscheinlich mit mehr oder weniger schwerwiegenden Konsequenzen ausgesetzt ist. Von einem hohen Risiko spricht man bei einer hohen Wahrscheinlichkeit und einer starken Bedrohung, von einem geringen Risiko, diese sich in Grenzen halten. Bei der Risikoanalyse werden die Wahrscheinlichkeiten und Auswirkungen der verschiedenen Bedrohungen voneinander unabhängig bewertet und daraus Gesamtkonsequenzen gezogen. Zur Veranschaulichung: Ein „Hochwasserrisiko" wird sowohl anhand der Wahrscheinlichkeit des Auftretens von Hochwasser (Überschwemmungsgebiete), als auch abhängig vom betroffenen Gebiet berechnet, beispielsweise, ob es dicht besiedelt ist oder nicht. So wird das Hochwasserrisiko in einem überschwemmungsgefährdeten, aber sehr dünn besiedelten Gebiet als etwa gleich hoch angesehen wie in einem nicht überschwemmungsgefährdeten, aber sehr dicht besiedelten Gebiet (wobei „nicht überschwemmungsgefährdet" bedeutet, dass die Wahrscheinlichkeit, überschwemmt zu werden, gering, aber nicht gleich null ist). Die Risikominderung kann deshalb sowohl über eine Begrenzung der Auswirkungen als auch der Wahrscheinlichkeit erfolgen. Bei einem Hochwasserrisiko kann man Wasserläufe kanalisieren, Wehre und Rückhaltebecken bauen (um die Eintretenswahrscheinlichkeit zu reduzieren), oder Dämme aufschütten, um die Häuser zu schützen, Bauten auf Pfählen bevorzugen oder Menschenansammlungen in Überschwemmungsgebieten vermeiden (um die Auswirkungen zu begrenzen).[13]

[11] https://www.mitre.org/our-impact/intellectual-property/crown-jewels-analysis

[12] https://www.merriam-webster.com/dictionary/phishing

[13] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

SCADA

„Supervisory Control And Data Acquisition“ (System zur Überwachung, Steuerung und Datenerfassung). Ein SCADA-System ist ein weiträumig angelegtes Fernmanagementsystem, mit dem eine große Zahl von Telemetriedaten in Echtzeit verarbeitet und technische Anlagen ferngesteuert werden können. Es handelt sich um eine Industrietechnologie im Bereich der Instrumentierung. Für die Cybersicherheit sind diese Systeme eine große Herausforderung, da es sich um Geräte handelt, die mit einem Netzwerk verbunden sind, und die einer Person, wenn diese die Kontrolle über sie übernimmt, die Steuerung der ihr zugrunde liegenden technischen Anlagen ermöglicht.

Schwachstelle

Schwachstellen in einem Informationssystem, in dessen Sicherheitsvorschriften, bei den internen Kontrollen oder bei der Implementierung, die von einer Bedrohungsquelle böswillig für die Auslösung eines Cyberangriffs genutzt werden könnten.

Security Operations Center (SOC)

Un Bei einem Security Operation Center (SOC) handelt es sich um eine Abteilung innerhalb einer Organisation mit der Aufgabe, IT-Sicherheitsoperationen zu zentralisieren. Sie kann bei den Beschäftigten der Organisation eingreifen[14].

Social Engineering

Social Engineering umfasst alle Techniken, die dazu dienen, eine Zielperson zur Preisegabe spezifischer Informationen oder zur Ausführung spezifischer illegaler Handlungen zu überreden.[15]

Speicherprogrammierbare Steuerung (SPS) / Programmable Logic Controller (PLC)

Programmierbare digitale elektronische Einrichtung zur Steuerung von Industrieprozessen durch sequenzielle Verarbeitung. Sie sendet auf der Basis von Eingangsdaten (Sensoren), Vorgaben bzw. Computerprogrammen Befehle an (Vor)Aktuatoren. SPS werden großflächig in fast allen Industrieprozessen Verwendung[16].

Spoofing

Im Zusammenhang mit der Cybersicherheit bezeichnet Spoofing eine Reihe von Techniken, mit denen eine Zielperson bezüglich der tatsächlichen Herkunft einer ihr übermittelten Information getäuscht wird. Je nach verwendeter Technik spricht man auch von missbräuchlich verwendeter Identität, Maskierung, Substitution usw.

WEP/WPA/WPA2/WPA3

Diese Akronyme stehen für Protokolle zur Sicherung des Zugangs zu einem drahtlosen Netzwerk (Wi-Fi). WEP (Wired Equivalent Privacy) wurde 1999 eingeführt. Dieses Protokoll war sehr schlecht gesichert, weshalb 2003 WPA (Wi-Fi Protected Access) als Ersatz dafür entwickelt wurde. Dieses wurde wiederum 2004 durch WPA2 ersetzt, das auf der Norm 802.11i des Institute of Electrical an Electronics Engineers (IEEE) basiert. 2017 wurde dann WPA3 veröffentlicht, das jedoch mehr als eine einfache Weiterentwicklung von WPA2 darstellt, das (noch) nicht überholt ist und auch 2023 noch weitreichend genutzt wird. WPA2 gibt es in zwei Versionen: Einerseits die Version WPA2 „Personal“ (auch WPA2-PSK - Pre-shard Key genannt), die auf einem gemeinsamen Schlüssel beruht und für den privaten Gebrauch zu Hause, in der Familie oder in einer sehr kleinen Einrichtung vorgesehen ist. Andererseits die Version WPA2 „Enterprise“, die auf einer RADIUS-Authentifizierung beruht (Mehrere Nutzer mit unterschiedlichen Konten) und für den Einsatz in Unternehmen vorgesehen ist. Es wird darauf hingewiesen, dass WPA2-PSK die Verwendung von zwei Verschlüsselungsalgorithmen zulässt: AES und TKIP, wobei der AES-Algorithmus sicherer ist.

[14] https://www.trellix.com/en-us/security-awareness/operations/what-is-soc.html

[15] https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

[16] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Bildnachweis

Bilder, mit freundlicher Genehmigung des Europäischen Verbandes der Binnenhäfen (EVB)
S 28 : © Steve Haider
S 45 : © Patrik Walde, patrikwalde.com
S 46 : © AZS Group Bonn
S 58 : © Hafen Düsseldorf

Shutterstock
Adobe stock

Künstlerische Leitung & Layout: Agentur dot. Deloitte Frankreich

Europäischer Ausschuss für die Ausarbeitung von Standards im Bereich der Binnenschifffahrt (CESNI)
Sekretariat der Zentralkommission für die Rheinschifffahrt (ZKR)
2 Place de la République – CS10023
F-67082 Strasbourg cedex
Frankreich
comite_cesni@cesni.eu
https://www.cesni.eu

In Partnerschaft mit dem Europäischen Verband der Binnenhäfen (EFIP)
The European Port House
Treurenberg 6
B-1000 Brüssel
Belgien