Journal für Mobilität und Verkehr
ISSN 2628-4154
www.dvwg.de

Cyber-Security – neue Herausforderung im Hafenmanagement

Andrea Vasterling-Will, Iven Krämer*
Der Senator für Wirtschaft, Arbeit und Häfen, Zweite Schlachtpforte 3, 28195 Bremen, Deutschland

Abstract

Schleusentore verweigern ihren Dienst, Kommunikationssysteme werden gestört oder fallen aus, komplexe Terminal-Steuerungssysteme weisen Fehlfunktionen auf, Schiffe, Trucks und Züge können nicht mehr be- und entladen werden. Szenarien wie diese mit ihren negativen Folgen für die intensiv vernetzten maritimen Logistikketten sind real. Cyber-Attacken stellen eine neue, rasant an Bedeutung gewinnende Gefahr für Häfen und Schifffahrt dar. Wie dieser Herausforderung im Hafenmanagement begegnet wird, ist Gegenstand dieser Analyse.

Schlagwörter/Keywords:
Hafensicherheit, Cyber-Security, Kritische Infrastruktur, Hafenmnagement

Einleitung

Nachdem die Gefahrenabwehr im Hafenmanagement bis zum Jahr 2004 aufgrund fehlender Bedrohungen und Vorgaben nur eine vergleichsweise geringe Bedeutung hatte bzw. wenn, dann auf das Aufgabenfeld der Arbeitssicherheit fokussiert war, änderte sich diese Situation schlagartig nach den terroristischen Angriffen vom 11. September 2001. In dessen Folge wurden neue Sicherheitsanforderungen an Häfen und Schifffahrt definiert und rechtsverbindlich geregelt. Dies machte im Hafenmanagement neue Strukturen, zusätzliche Aufgaben und Personal erforderlich. Nach fast fünfzehn Jahren Erfahrung zeigt sich, dass dieser Herausforderung in den deutschen Häfen insgesamt gut begegnet werden konnte und die inzwischen etablierten Akteure und Organisationen sämtliche Themen der physischen Hafensicherheit wie Umzäunungen, Zugangskontrollen, Personenvereinzelungsanlagen, Schranken, Kameraüberwachungen und ähnliches hoch professionell regeln.

Einer neuen, rasant an Bedeutung gewinnenden Gefahr durch Störungen und Manipulationen der IT-Infrastrukturen von Häfen und Unternehmen aber werden diese Strukturen nicht gerecht. Immer mehr Cyber-Angriffe auf Häfen und Schifffahrt mit zum Teil erheblichen logistischen wie finanziellen Schäden zeigen dies eindrücklich. In der Konsequenz müssen sich die Häfen und das Hafenmanagement zügig der Bedrohungslage stellen und sowohl fachlich wie organisatorisch-strukturell Abwehrstrategien entwickeln. Dieser Beitrag beschreibt dazu den aktuellen Status und die Entwicklungen von Cyber-Security als neuer Herausforderung im Hafenmanagement.

Gefahrenabwehr – grundlegend neue Aufgabenstellung seit 2004

In der Zeit vor 2004 war es nicht nur für die Hafenarbeiter und autorisierte Personen, sondern auch für interessierte Besucherinnen und Besucher ohne größere Schwierigkeiten möglich, in vielen Hafengebieten bis an die Kajen und an die Schiffe zu gelangen und dort den Hafenumschlag und die logistischen Aktivitäten aus nächster Nähe zu betrachten. Zugangsbeschränkte oder gar grundsätzlich abgesperrte Bereiche gab es nur wenige und das Betreten des Hafengebietes erfolgte lediglich auf eigene Gefahr. Dann aber erfolgten die terroristischen Anschläge von New York und Washington am 11. September 2001, die in der Folge zu gravierenden Veränderungen auf dem Gebiet des Gefahrenabwehrrechts geführt haben. Betroffen waren neben dem Luftverkehr insbesondere auch Häfen und die Schifffahrt. Schiffe in der internationalen Fahrt waren dabei sowohl als Bedrohungsobjekte als auch als potenzielle Tatwerkzeuge für terroristische Zwecke

* Korrespondierender Autor.
E-Mail: iven.kraemer@wah.bremen.de (I. Krämer)

identifiziert worden, so dass die Schnittstelle Schiff/Hafen in den Focus der Sicherungsmaßnahmen gerückt worden ist.

Ein wesentlicher Schritt dafür erfolgte am 12. Dezember 2002 auf der diplomatischen Konferenz von London, bei der durch die International Maritime Organisation (IMO) eine grundlegende Änderung der *International Convention for the Safety of Life at Sea* (SOLAS) beschlossen wurde. Angefügt wurde ein neues Kapitel Xl-2 mit 13 Regeln zur Verbesserung der Gefahrenabwehr in der Schifffahrt und an Hafenanlagen und als Entschließung 2 zu diesem Kapitel wurde der *International Ship and Port Facility Security Code* (ISPS-Code) mit einem verbindlichen Teil A und einem empfehlenden Teil B ergänzt.

In der praktischen Ausgestaltung dessen ist auf europäischer Ebene am 31. März 2004 die Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates zur Erhöhung der Sicherheit auf Schiffen und in Hafenanlagen in Kraft getreten. Diese schreibt in den europäischen Häfen die Geltung des Teils A und gemäß Artikel 13 Abs. 5 der Verordnung auch von Teilen des Abschnittes B des ISPS-Codes verbindlich vor.

Mit der Richtlinie 65/2005/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 erfolgte eine Ergänzung der nach der Verordnung (EG) Nr. 725/2004 bereits getroffenen Maßnahmen. Die Richtlinie sieht eine räumliche Ausdehnung des landseitig geschützten Gebiets von den Hafenanlagen, als Schnittstellen zwischen Schiff und Küste, auf das gesamte Hafengebiet vor.

Beispiel: Umsetzung des ISPS-Codes in Bremen

Nach dem Grundgesetz steht dem Bund für den wasserseitigen Schutz die Gesetzgebungskompetenz zu. Für den landseitigen Schutz sind die Länder zuständig. In Bremen ist die erforderliche Umsetzung durch das erste Bremische Hafensicherheitsgesetz (BremHaSiG) vom 06. Juli 2004 erfolgt. Seitdem werden für ca. 60 Hafenanlagen in Bremen und Bremerhaven in regelmäßigen Abständen behördliche Risikobewertungen erarbeitet, auf deren Grundlage die jeweiligen Betreiber der Hafenanlagen einen Gefahrenabwehrplan erstellen. Dieser Gefahrenabwehrplan ist der zuständigen Behörde zur Genehmigung vorzulegen. Die in dem Plan beschriebenen Eigensicherungsmaßnahmen wie z. B. Umzäunungen des Betriebsgeländes, Zugangskontrollen, Personenvereinzelungsanlagen, Schranken oder Kameraüberwachung sind von den Anlagenbetreibern umzusetzen und unterliegen der Kontrolle der zuständigen Behörden. Ein freier Zugang wie in früheren Jahren üblich, ist dementsprechend seit 2004 nicht mehr gestattet. Jede ISPS-zertifizierte Hafenanlage hat einen Beauftragten für die Gefahrenabwehr, den Port Facility Security Officer (PFSO) zu benennen, der bestimmte Bedingungen erfüllen muss und im Unternehmen für die Gefahrenabwehr verantwortlich ist und Behörden gegenüber als Ansprechpartner auftritt.

Die Umsetzung der Richtlinie 65/2005/EG durch den Ausbau des Schutzregimes gegen terroristische Anschläge auf den Gesamthafen ist in Bremen in den §§ 4-7 BremHaSiG geregelt. Die dort umrissenen Aufgaben werden grundsätzlich als Staatsaufgabe verstanden. Die Risikobewertungen und Gefahrenabwehrpläne für den Gesamthafen werden von Behörden erstellt und ausgeführt. Privatpersonen haben lediglich Mitwirkungspflichten (z. B. zur Informationserteilung oder Zutrittsgewährung).

In der praktischen Ausgestaltung des ISPS Codes arbeiten in Bremen alle an dem Sicherungsprozess beteiligten Behörden, wie z. B. der Senator für Inneres, die Wasserschutzpolizei, der Hafenkapitän, das Hansestadt Bremische Hafenamt, die Umschlaggesellschaften, die Hafendienstleistungsunternehmen, Infrastrukturdienstleister sowie der Senator für Wirtschaft, Arbeit und Häfen eng zusammen. Es besteht einen regelmäßiger Austausch und feste Termine wie jährlich stattfindende Sitzungen des Hafensicherheitsausschuss oder Treffen der Sicherheitsbeauftragten der Unternehmen. Gemeinsam wird das Ziel verfolgt, die Gefahrenabwehr sachgerecht mit den bremischen Interessen an der Entwicklung der Hafenwirtschaft in Übereinstimmung zu bringen. Dabei ist eine sinnvolle Balance zwischen notwendigem Schutz einerseits und der Abwehr von Belastungen für die Wirtschaft sowie die Erhaltung von Freiräumen andererseits zu finden.

Störungen der IT-Infrastruktur – neues Bedrohungspotenzial für Häfen und Schifffahrt

Neben den physischen Bedrohungen wurden in jüngerer Zeit und mit erheblich steigender Tendenz Hackerangriffe auf diverse Infrastrukturträger und Wirtschaftsunternehmen bekannt, etwa auf Hafenterminals in Rotterdam, Antwerpen und San Diego oder auch auf diverse Reedereibetriebe. Der Weltmarktführer im Containertransport Maersk beispielsweise hat nach eigenen Angaben im Rahmen eines unspezifischen Cyberangriffs zuletzt rund 300 Mio. Euro Verlust erlitten und die Arbeit in vielen Terminals kam ganz oder teilweise zum Erliegen. Große Teile der unternehmenseigenen IT-Infrastruktur mussten innerhalb von wenigen Tagen ausgetauscht werden.

Dementsprechend sehen nicht nur Reedereien und Hafenbetreiber, sondern zunehmend auch die Verlader und Versicherungen in Cyber-Angriffen auf Schiffe und Häfen ein erhebliches Risiko, dessen Gefährdungspotenzial für globale Supply Chains inzwischen deutlich höher bewertet wird als das der internationalen Piraterie. Die verschiedenen Vorfälle haben eindrucksvoll dargestellt, welches Gefahrenpotential die weltweite Vernetzung von Computersystemen birgt und welche neuen Herausforderungen im Bereich der Gefahrenabwehr zu bewältigen sind. Fast täglich berichtet die Presse inzwischen von gravierenden Cyberangriffen. Durch die zunehmende Digitalisierung sind Kommunikations- und Geschäftsprozesse erheblich beschleunigt worden, gleichzeitig bieten sich Cyberangreifern aber auch vielfältige Möglichkeiten der Sabotage und des Datendiebstahls.

Das Bundesamt für Sicherheit in der Informationstechnik

(BSI) nimmt mit seinen Einrichtungen und Aktivitäten bereits zahlreiche Aufgaben zur Umsetzung der Cyber-Sicherheit in Deutschland wahr. Hierzu gehört u. a. auch der Schutz Kritischer Infrastrukturen. Nach der Definition des BSI sind Kritische Infrastrukturen (KRITIS) Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. So sind Betreiber kritischer Infrastrukturen angehalten, IT-Sicherheitsstandards einzuhalten und sicherheitsrelevante Vorfälle zu melden. Häfen sind aufgrund ihrer Komplexität und ihrer vielfältigen Akteurs-Beziehungen bislang nicht per se als kritische Infrastrukturen eingestuft, aber natürlich erfüllen sie ab einer bestimmen Größe und Vernetzung die genannten Kriterien.

Häfen im Blickfeld der Cyber-Security

In modernen Häfen wird die Abwicklung des Umschlags und der dazugehörigen Lager- und Transportbewegungen längst komplett digital gesteuert. Alle am Hafentransport beteiligten Akteure (wie z. B. Terminalbetreiber, Reeder, Spediteure, Betreiber von Hafen-IT, Bahn, Hafenbehörden und Zoll) sind in einem komplexen Verbund miteinander vernetzt und aufeinander angewiesen, weshalb sie kontinuierlich vielfältige Informationen und große Datenmengen untereinander austauschen.

Sollte es nach Darstellung des Institutes für Seeverkehrswirtschaft und Logistik in Bremen einem Angreifer gelingen, Teilnehmer des Verbundes zu werden – sei es durch einen Angriff auf das IT-System eines Hafenakteurs oder als Innentäter –, kann er manipulierte Nachrichten in das Gesamtsystem (Kommunikationsverbund) einzuspielen versuchen, die auf den ersten Blick korrekt aussehen. Diese Nachrichten erscheinen dann den einzelnen Hafenanwendungen plausibel und werden entsprechend weiterverarbeitet. Selbst wenn die einzelnen Systeme der Hafenakteure nach dem Stand der Technik abgesichert sind, bedeutet das nicht automatisch, dass der gesamte Hafenkommunikationsverbund im Zusammenspiel sicher ist, und das vor dem Hintergrund, dass IT-Angriffe in Zukunft immer raffinierter werden. Deshalb ist ein Schutz in vielerlei Richtungen unerlässlich. Besonders gravierend wäre ein Ausfall der Hafeninfrastruktur durch Sabotage, der zu Versorgungsengpässen bei der Bevölkerung führen könnte. Schließlich werden mehr als 90 Prozent der weltweit gehandelten Güter auf dem Seeweg transportiert.

Organisatorische Maßnahmen zur Cyber-Abwehr in den Häfen

Angesicht der wachsenden Cyber-Gefährdung ist zu beobachten, dass immer mehr Hafen- und Logistikakteure wie Reedereien, Terminalbetriebe und Hafenmanagementgesellschaften der neuen Form der Bedrohung mit organisatorischen Anpassungen und zum Teil auch neuen Strukturen begegnen. Der ISPS-Code verlangt zwar bereits, dass bei der Risikobewertung von Hafenanlagen auch die IT-Infrastruktur der Unternehmen betrachtet werden soll. Weitere konkretere Maßnahmen sieht der ISPS-Code bislang jedoch nicht vor. Aktuell werden im internationalen Rahmen wie auf der IMO-Ebene Richtlinien für die maritime Wirtschaft erarbeitet, die sich mit der Cybersicherheit beschäftigen. So hat der Schiffssicherheitsausschuss MSC im Juni 2018 gemeinsam mit dem FAL-Ausschuss Richtlinien betreffend Cybersicherheit erlassen (MSC-FAL.1/circ.3). Diese Vorgaben sind zunächst jedoch nicht verbindlich, sondern haben nur empfehlenden Charakter und die IMO beabsichtigt zunächst, die Umsetzung der empfehlenden Vorgaben abzuwarten.

Aus Hafenperspektive ist der inhaltliche Handlungsbedarf zur Cyber-Security seit den o. g. Vorfällen allerdings unumstritten. Der Hafen von Rotterdam beispielsweise hat in diesem Kontext im Hafenmanagement bereits seit 2017 eine zentrale Stelle für Cybersicherheit eingerichtet. Diese wurde beim Hafenamt organisatorisch angebunden und dem Aufgabenbereich des Hafenkapitäns zugeordnet. Ebenso hat der Hafen von Amsterdam in 2018 bekannt gegeben, ein Cyber Security-Programm mit einer Hotline installiert zu haben, um frühzeitig vor digitalen Bedrohungen Kenntnis zu erhalten und Informationen mit den am Netzwerk beteiligten Firmen auszutauschen. Die zuständige Hafenmeisterin wird dabei mit den Worten zitiert: Cyberattacken sind nicht durch physische Grenzen aufzuhalten.

Auch der Senator für Wirtschaft, Arbeit und Häfen der Freien Hansestadt Bremen als zuständige Behörde für das Thema Hafensicherheit hat sich aktiv mit der Herausforderung Cyber Security befasst und dafür gesorgt, dass ab 2019 die Funktion eines Port Cyber Resilience Officers für die bremischen Häfen bei der städtischen Hafenmanagementgesellschaft bremenports eingerichtet wird. Aufgabe ist es, die Thematik der Cyber-Security inhaltlich zu verfolgen und als zentrale Ansprechstelle für interne und externe Fragen zur Verfügung zu stehen. Zudem soll der Port Cyber Resilience Officer für die Unternehmen im Hafen und im Transportsektor eine koordinierende Funktion zur Thematik übernehmen. Ebenso hat Niedersachsen mit Beginn des Jahres 2019 die Stelle eines Port Cyber Security Officers eingerichtet und in Hamburg werden innerhalb der Hamburg Port Authority ähnliche Aufgaben wahrgenommen.

Die beschriebenen Aktivitäten zeigen trotz der noch fehlenden bzw. nicht abschließenden rechtlichen Vorgaben und Verpflichtungen, dass in den Häfen grundsätzlich vergleichbare Ansatzpunkte zum Umgang mit Cyber-Bedrohungen bestehen. Es ist davon auszugehen, dass sich diese Ansatzpunkte anhand der Anforderungen weiterentwickeln werden, wobei eine enge Zusammenarbeit und ein gezielter Austausch unter den Port-Cyber-Spezialisten auf nationaler und europäischer Ebene sinnvoll sein wird.

Cyber-Security in Häfen und Schifffahrt als Forschungsgegenstand

Im Oktober 2018 ist in Bremerhaven das ***Institut für den Schutz maritimer Infrastrukturen*** des Deutschen Zentrums für Luft-und Raumfahrt (DLR) eröffnet worden. Vor dem Hintergrund von Energiewende, Digitalisierung, innovativer Mobilität und globaler Vernetzung widmet sich das neue Institut der Aufgabe, die dafür notwendigen Infrastrukturen wie Häfen und Offshore-Windanlagen vor Unfällen, terroristischen oder anderen Angriffen zu schützen. Es ist europaweit das erste Institut seiner Art. Die Einrichtung wird bei seiner Arbeit unter anderem eng mit der Bundespolizei und mit weiteren Behörden und Organisationen mit Sicherheitsaufgaben, aber auch mit Nichtregierungsorganisationen wie der Deutschen Gesellschaft zur Rettung Schiffbrüchiger und der Wirtschaft zusammenarbeiten.

Bremen hat in den zurückliegenden Jahren im Kontext der Digitalisierung im Bereich Forschung und Entwicklung hohe Kompetenz aufbauen können. Dementsprechend verfolgen die Unternehmen und Forschungseinrichtungen im Land Bremen bereits heute eine Vielzahl von zum Themenbereich der Digitalisierung gehörenden Ideen, Projekten und Maßnahmen (Fördermittelgeber sind verschiedene Bundesministerien und/oder die EU). Mit Bezug zum Thema Hafensicherheit bzw. Sicherung der Lieferkette zählen unter anderem folgende Projekte:

SecProPort läuft seit November 2018 für die Dauer von drei Jahren im Auftrag des Bundesministeriums für Verkehr und digitale Infrastruktur im Rahmen des Förderprogramms IHATEC. Neben der BLG Logistics Group, dem Institut für Seeverkehrswirtschaft und Logistik (ISL) und der Universität Bremen sind noch die dbh Logistics, die Reederei Hapag Lloyd, die Duisburger Hafen AG, das Deutsche Forschungszentrum für Künstliche Intelligenz und die Firma Datenschutz CERT an dem mit rd. 2,8 Mio. Euro geförderten Projekt beteiligt. Mit den verschiedenen Partnern aus dem gesamten Tätigkeitsfeld der Hafenlogistik soll anhand einer Prozess- und Bedrohungsanalyse eine übergreifende Sicherheitsarchitektur für den Kommunikationsverbund im und um den Hafen entwickelt werden. In besonderem Blickfeld stehen dabei die Datenschnittstellen, die häufig ein Ziel von Hackerangriffen darstellen. Zudem sollen Maßnahmen entwickelt werden, die im Schadensfall die Auswirkungen auf andere Akteure des Verbunds minimieren und das betroffene Netz in kontrollierter Weise wieder in den Normalzustand zurückführen.

PortSec- IT-Risikomanagement in der Hafentelematik - Ziel des Verbundprojekts PortSec ist die Erforschung eines systematischen und umfassenden IT-Risikomanagements in der Hafentelematik. Die Heterogenität der Software in den verschiedenen Systemen der beteiligten Unternehmen und Behörden und deren Interaktionen bergen spezifische IT-Sicherheitsrisiken, die es zu identifizieren gilt. Die Verbundkoordination lag beim Institut für Seeverkehrswirtschaft und Logistik, Partner waren die dbh Logistics IT AG, datenschutz cert GmbH und die Universität Bremen. (01.09.2016 – 01.08.2018, Volumen 1,68 Mio. €, davon 76 % Förderanteil, KMU-innovativ, BMBF).

Im Kontext der Hafensicherheit war Bremen an nationalen und internationalen Forschungsvorhaben, wie beispielsweise ***ECSIT, CASSANDRA und CORE*** beteiligt. Ziel des EU-Projektes CASSANDRA (Common Assessment and Analysis of Risk in Global Supply Chains) war eine Erhöhung der Sicherheit internationaler Containertransportbewegungen durch Optimierung der Sichtbarkeit vorhandener Informationen. Dazu wurde im Zeitraum Juni 2011 bis Mai 2014 ein Data-Sharing-Konzept entwickelt, das sowohl Wirtschaft als auch Behörden eine erweiterte Bewertung der Risiken erlaubt. Darüber hinaus war Bremen als Partner an dem EU-Projekt CORE (Consistently Optimised Resilient Secure Global Supply Chains) beteiligt, welches über einen Zeitraum von vier Jahren lief und im März 2018 endete. CORE ist eines der bislang größten europäischen Forschungs- und Demonstrationsvorhaben mit rund 70 Partnern. Das Projekt hat gezeigt, wie der Schutz und die Sicherung der globalen Lieferkette sowie eine Verringerung Störungsanfälligkeiten erreicht werden kann. Weiterhin ist das Projekt ***MITIGATE*** zu nennen, wobei es um die Untersuchung kritischer IT-Schnittstellen geht. Entwickelt wurde eine dynamische, modulare Softwarelösung, die sowohl die Erkennung als auch die Analyse und die Bewertung von möglichen Sicherheitslücken leistet. Bremen war hier aktiv durch die dbh Logistics IT AG vertreten. Zudem unterstützen die zuständigen Stellen der Hafensicherheit diverse Sicherheitsprojekte durch Bereitstellen von Informationen bzw. durch Interviews, wie aktuell beim Sicherheitsprojekt ***LOMA***, wo es um die Ermöglichung der Erstellung automatischer Lagebilder geht.

Fazit

Ausgehend von der Analyse und Beschreibung der Cyber-Security als neuem Handlungsfeld der Hafensicherheit kann eindeutig festgestellt werden, dass die weiter fortschreitende Digitalisierung und Vernetzung zu einer ebenso weiter wachsenden Angreifbarkeit von Häfen und internationalen Transportketten führen wird. Die Bedrohungsszenarien werden sich weiterentwickeln, so dass den neuen Herausforderungen nur in enger Zusammenarbeit und Abstimmung zu begegnen ist. Sowohl auf Länderebene als auch beim Bund und der Europäischen Union sind Kommunikation und Austausch zu stärken, die Kompetenzen im Bereich Cyber-Security zu erhöhen und aufeinander abgestimmte, vielleicht sogar gemeinsame Strategie zu entwickeln. Verbunden sein wird diese Entwicklung mit der Festlegung von Standards und rechtlichen Vorgaben, wozu von Seiten der Häfen bereits jetzt durch die Schaffung erster Strukturen und die Umsetzung organisatorischer Maßnahmen wichtige Vorarbeiten geleistet werden.