Cybersicherheit für die Schifffahrt – mit einer Schiffsbrücke als Test- und Entwicklungslabor

***Zusammenfassung*—Angriffe auf kritische Infrastrukturen, wie zum Beispiel auf die Energieversorgung, die Informations- und Kommunikationstechnologie, aber auch auf die Transport- und Logistikbranche finden nicht erst seit heute auch im Cyberspace statt. Die geopolitischen Veränderungen der letzten Zeit haben die Verletzlichkeit dieser Infrastrukturen jedoch besonders deutlich gemacht. Dies gilt auch für die maritime Logistik, beziehungsweise Schiffe als deren unverzichtbares Rückgrat. Die fortschreitende Digitalisierung und Vernetzung der Systeme an Bord von Schiffen erfordern daher Maßnahmen, mit dem erhöhten Risiko für Cyberangriffe umzugehen. Diese Maßnahmen umfassen nicht nur die Entwicklung geeigneter Schutzmaßnahmen, sondern auch Methoden zur Erkennung von Angriffen, zur gründlichen Erprobung existierender Komponenten auf der Brücke und im Maschinenraum, und zu speziellem Training für die Schiffsbesatzung. Für all diese Aspekte ist eine Testumgebung von Vorteil, welche die echten Bedingungen möglichst originalgetreu abbildet und es ermöglicht, Cyberangriffe einfach und benutzerfreundlich durchzuspielen. Trotz des Bedarfs für eine solche Umgebung sind "Trainingsplätze", die solche Anforderungen erfüllen, nur spärlich gesät. Es wird deshalb ein Labor präsentiert, das reale Schiffsbrücken-Hardware mitsamt dazugehöriger Antennenplattform mit digitalen Hilfsmitteln kombiniert, um Test- und Trainingsszenarien für die maritime Cybersicherheit zu entwickeln. Darin wird untersucht, wie die Schiffsbrücke cybersicher gestaltet werden kann.**

I. Cybersicherheit im maritimen Umfeld

Die maritime Logistik bildet das Rückgrat der globalen Wirtschaft – der mit Abstand größte Teil des Welthandels findet über den Seeweg statt [1], [2]. Da fast zwei Drittel der weltweiten Versorgung mit Erdöl und anderen flüssigen Energieträgern per Schiff transportiert werden, sind die meisten globalen Lieferketten vom maritimen Sektor abhängig. Nachdem in Deutschland Erdgasimporte über den Seeweg die Lieferungen aus Russland ersetzen sollen, wird diese Abhängigkeit in Zukunft eher noch stärker. Dahingehend wurden auch LNG-Terminals kürzlich als kritische Infrastruktur eingestuft[1]. Aber auch die LNG-Tanker sind für die Versorgung kritisch – insbesondere unter dem Gesichtspunkt, dass davon im Moment weltweit lediglich etwa 640 zur Verfügung stehen [3].

Die insgesamt fortschreitende Vernetzung und Abhängigkeit von digitalen Technologien stellt jedoch eine große Angriffsfläche für Cyberattacken dar, nicht nur für Unternehmen an Land, sondern auch für alle möglichen Schiffstypen. Solche Angriffe können direkt auf Brücken- oder Navigationssysteme gezielt sein, oder diese zufällig treffen. Beide Fälle können zu schweren Konsequenzen für die Schiffsbesatzung, die Umwelt oder sogar für die globale Wirtschaft führen – beispielsweise im Falle einer Blockade des Suezkanals wie durch die *Ever Given* im März 2021.

[1]s. Dritte Verordnung zur Änderung der BSI-Kritisverordnung (BGBl. 2023 I Nr. 53 vom 01.03.2023)

Schwachstellen zu identifizieren, Cybervorfälle zu erkennen und angemessen darauf zu reagieren ist daher wesentlich für einen sicheren Schiffsbetrieb. Um diesen Herausforderungen zu begegnen hat die IMO die Regierungen der Mitgliedsländer aufgefordert, Cybersicherheit ab spätestens 2021 in den Safety Management Systems (SMSs) zu behandeln [4]. Im International Safety Management Code (ISM-Code), also den Vorschriften für einen sicheren Schiffsbetrieb, werden Cyberrisiken mit den "klassischen" Risiken gleichgestellt. Dies macht die Entwicklung von Vorgehensweisen und Maßnahmen für wirkungsvolle Reaktionen auf Cyberangriffe erforderlich.

Die International Association of Classification Societies (IACS) hat umfangreiche Vorschriften veröffentlicht, die ab Januar 2024 für die Klassifizierung von Schiffsneubauten verpflichtend sein werden [5], [6]. Diese Anforderungen verlangen die Einbeziehung von Aspekten der Cybersicherheit praktisch über die gesamte Lebensdauer des Schiffes, das heißt ab der Entwicklungsphase.

Allerdings haben Schiffe eine sehr lange Lebensdauer. Momentan ist die globale Handelsflotte im Schnitt 22 Jahre alt [7] und viele dieser Schiffe werden mindestens noch über das nächste Jahrzehnt hinweg in Betrieb sein. Zu deren Bauzeit fand die Cybersicherheit häufig noch keine Beachtung. Um also eine Strategie für die maritime Cybersicherheit [8] erfolgreich und wirkungsvoll gestalten zu können, muss diese jeweils auf das bestimmte Alter eines Schiffes und seiner Systeme abgestimmt sein.

Obwohl der Trend zu autonomen Fahrzeugen auch den maritimen Sektor ergriffen hat, wird die bemannte Schifffahrt in den nächsten Jahrzehnten weiterhin die vorherrschende Rolle spielen [7], [9]. Der Ausbildung von Seefahrern mangelt es jedoch bisher an Aufmerksamkeit für die Cybersicherheit [10]. Inwiefern solche Aspekte in das STCW-Übereinkommen, also in die Ausbildung von Seeleuten integriert werden sollten, wird momentan noch diskutiert.

II. Angriffsszenarien

Es ist nur in wenigen Fällen vorgeschrieben, Cybervorfälle an Behörden zu melden [11]; eine universelle Verpflichtung dazu besteht nicht. Die Anzahl der ungemeldeten Vorfälle ist also vermutlich sehr hoch. Doch auch auf anderen Wegen lässt sich ein Zuwachs an Cybervorfällen in den letzten Jahren bestätigen – beispielsweise durch Berichte von Mitarbeitern und Beratungsfirmen aus der Branche, der Anzahl von Stellenausschreibungen maritimer Firmen im Bereich Cybersecurity, oder wissenschaftlichen Beiträgen auf diesem Gebiet [12].

Betrachten wir die Typen der bekannt gewordenen Cybervorfälle, dann fällt auf, dass knapp die Hälfte davon (47 %) auf Infektionen mit Viren oder Malware zurückzuführen ist [13].

Abbildung 1. Labor-Schiffsbrücke mit Radar, ECDIS, AIS, GNSS, und VDR.

Weitere 39 % sind "konventionelle" Cyberangriffe, wie z.B. Denial of Service (DoS)-Attacken. Es lässt sich annehmen, dass ein Großteil dieser Angriffe ungeschützte Dienste oder Schnittstellen betreffen, die eher zufällig durch ungezielte Malware "getroffen" werden und nicht speziell gegen konkrete maritime Geräte gerichtet sind.

Funk-basierte Angriffe zur Störung und Manipulation des Globalen Navigations-Satelliten-Systems (GNSS) oder dem Automatic Identification System (AIS) dagegen machen nur etwa 4 % der Vorfälle aus, beinhalten jedoch aufwändige und gefährliche Angriffe aus dem elektromagnetischen Spektrum gegen die Sensoren eines Schiffes, oder das Integriertes Brückensystem (IBS) selbst. Für die Untersuchung solcher Angriffe sind bisher nur wenige Testumgebungen vorhanden.

Was in existierenden Testumgebungen ebenso wenig Beachtung findet, sind Attacken, die sich den menschlichen Faktor direkt zunutze machen. Dies umfasst zum Beispiel *Social Engineering* durch das Sammeln von persönlichen Informationen über soziale Medien oder Phishing, aber auch Bedienungsfehler oder vorsätzliche Handlungen mit böswilliger Absicht. Meist sind diese Techniken und Vorkommnisse jedoch nur der erste Schritt zur Vorbereitung im Rahmen einer sogenannten Kill-Chain, also eines größeren, komplexer angelegten Angriffs, sodass viele dieser Vorfälle letztendlich anderen Kategorien zugeordnet werden. Dies wäre zum Beispiel der Fall, wenn ein argloser oder böswilliger Benutzer ein beschädigtes Medium an ein Brückensystem anschließt und dadurch mit Malware infiziert, sodass es im Anschluss für eine DoS-Attacke ausgenutzt werden kann. Folglich dürfen durch menschliche Fehler ausgelöste Cybervorfälle, auch wenn sie lediglich einen geringen Teil der erfassten Angriffe (beispielsweise 6 % in der ADMIRAL-Datenbank [13]) ausmachen, keinesfalls in Testumgebungen außer Acht gelassen werden.

In der Schifffahrt, und insbesondere auf der Brücke, kommt als menschlicher Faktor noch der Stress in kritischen Situationen, sowie häufig damit einhergehend die Übermüdung der Seeleute hinzu [14]. Dabei lassen viele Situationen nur wenig Raum für Fehler. Für die Havarie der *Ever Given* im Suezkanal waren Verständigungsprobleme und widersprüchliche Angaben der Lotsen mitursächlich [15] – und nur wenige Minuten Verwirrung waren ausreichend, den Welthandel über mehrere Tage zu blockieren. Es ist nicht schwer sich vorzustellen, dass diese Verwirrung beim nächsten Mal nicht durch schwierige Wetterbedingungen, sondern durch fehlerhafte und widersprüchliche Geräteanzeigen aufgrund eines Cyberangriffs ausgelöst werden könnte. Deshalb ist es essentiell, Cyberangriffe möglichst frühzeitig zu erkennen, sodass die Schiffsbesatzung angemessen darauf reagieren kann.

III. Test- und Entwicklungsumgebung

Es bedarf also einer Umgebung, um Cyberangriffe auf ein Schiff zu simulieren, um den Umgang mit und die Abwehr von solchen Angriffen auf technischer und menschlicher Ebene zu untersuchen und zu trainieren.

Um diese Problematik anzugehen, bietet sich unser *Maritimes Cybersicherheits-Labor* an. Einerseits ist dieses mit denselben Hardwarekomponenten eines IBS ausgestattet wie ein reguläres Schiff (vgl. Abbildung 1); die Komponenten wurden dabei gemäß den Vorgaben der Klassifizierungsgesellschaften eingebaut. Andererseits umfasst es ein Portfolio an Softwarelösungen, die es ermöglichen, Cyberangriffe auf die Hardware tatsächlich durchzuführen.

Die Verwendung echter Hardwareermöglicht es Forschern, Entwicklern und Anwendern aus dem maritimen Bereich gleichermaßen, zugeschnittene Cyberangriffe durchzuführen und in einer kontrollierten Umgebung zu untersuchen und auszuwerten. Und das, ohne ein Schiff dafür in die Werft schicken zu müssen.

Die Softwarelösungen dienen dabei sowohl der einfachen Durchführung von Angriffen, als auch der Entwicklung reproduzierbarer Testszenarien. Dadurch soll die Aufmerksamkeit des maritimen Personals gegenüber den Auswirkungen von Cyberrisiken geweckt werden. So können gemeinsam Reaktionsstrategien entwickelt und das erarbeitete Verhalten im Falle eines Cyberangriffs eingeübt werden.

Die verfügbaren Geräte auf der Antennenplattform und dem IBS, sowie deren Verbindung untereinander, sind in Abbildung 2 schematisch dargestellt. Dazu zählen Anlagen für den Seefunk, die Satellitenkommunikation, die Satellitennavigation, sowie für AIS und NAVTEX. Zusätzlich befindet sich eine Radarantenne auf der Plattform. Diese Anlagen können, wie bei einem richtigen Schiff, von der Brücke aus bedient werden und rund um die Uhr Realdaten aus der Hafenumgebung liefern. Die Brücke verfügt zudem noch über ein Electronic Chart Display and Information System (ECDIS), sowie einen Voyage Data Recorder (VDR).

Als Testumgebung dient ein virtualisiertes Labor, welches die Simulation und Analyse maritimer Cyberattacken und deren Auswirkungen ermöglicht. Dieses beinhaltet:

- einem Tool, welches Angriffe über das brückeninterne Netzwerk ausführen oder simulieren und dadurch die Effektivität von Gegenmaßnahmen evaluieren kann,
- einem Programm zur Verarbeitung, Visualisierung und Analyse des Netzwerkverkehrs,
- und einem Intrusion Detection System (IDS), das auch eine auf die Schiffscrew zugeschnittene Benutzerschnittsstelle beinhaltet.

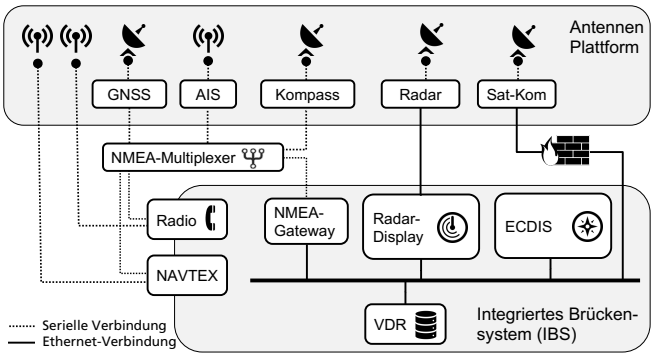

Abbildung 2. Verfügbare Hardwarekomponenten und Netzwerkarchitektur der Verbindung von Antennenplattform mit IBS.

Ziel ist es nun, diese beiden Komponenten miteinander zu kombinieren. Die Verbindung der Softwaretools mit der Hardware ermöglicht insbesondere die Untersuchung der schiffsspezifischen Angriffsszenarien aus Abschnitt II, wie dies nur in wenigen bereits existierenden Testumgebungen möglich ist.

IV. Auswertung der Ergebnisse

Die Durchführung spezieller Trainings in einer so realistischen Umgebung bietet die Möglichkeit, direktes Feedback des maritimen Personals zu erhalten. Damit können die digitalen Werkzeuge angepasst und verbessert werden. Zudem kann es auch dabei unterstützen, gemeinsam mit den Benutzern Empfehlungen für die Reaktion auf einen Cyberangriff zu erarbeiten und auszutesten.

Dazu werden die Hardware- und Softwarekomponenten momentan zusammengeführt. Dabei fanden bereits erste Tests statt. Beispielsweise ist es erfolgreich gelungen, einen Angriff auf das echte Radargerät zu simulieren. Es steht zu erwarten, dass bis zum Einsendeschluss der Langfassung hier bereits erste Testergebnisse aus der praktischen Anwendung vorliegen.

Literatur

[1] G. C. Kessler and S. D. Shepard, *Maritime Cybersecurity: A Guide for Leaders and Managers*, 2nd ed. Daytona Beach, FL, USA: independently published, 2022.

[2] Umweltbundesamt, "Fakten zur Seeschifffahrt und zu ihren Auswirkungen auf die Umwelt," https://www.umweltbundesamt.de/themen/wasser/gewaesser/meere/nutzung-belastungen/schifffahrt#fakten-zur-seeschifffahrt-und-zu-ihren-auswirkungen-auf-die-umwelt, Mar. 2023.

[3] G. Höhler, "Die schwierige Suche nach genügend Flüssiggastankern," website, Aug. 2022. [Online]. Available: https://www.rnd.de/politik/lng-engpaesse-bei-fluessiggas-tankern-und-kaum-besserung-in-sicht-LQGDZ343HRFDZM75J6M75NZCZA.html

[4] IMO MSC.428(98), "Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems," June 2017.

[5] IACS-UR-E26, "E26 – Cyber resilience of ships," IACS Req., Apr. 2022.

[6] IACS-UR-E27, "E27 – Cyber resilience of on-board systems and equipment," IACS Req., Apr. 2022.

[7] United Nations Conference on Trade and Development (UNCTAD), "Review of Maritime Transport 2022," New York, NY, USA, 2022.

[8] A. Hahn, M. Steidel, S. Berner, A. Nies, G. S. Schaal, and A. Weiß, "Roadmap Sichere Digitale Küste 2030," https://www.emaritime.de/wp-content/uploads/2021/12/OFFIS_A4_Roadmap_Digital.pdf, Institut für Informatik OFFIS e.V., Tech. Rep., 2021.

[9] C. Wienberg, "Maersk's CEO Can't Imagine Self-Sailing Box Ships in His Lifetime," Feb. 2018, https://www.bloomberg.com/news/articles/2018-02-15/maersk-ceo-can-t-imagine-self-sailing-box-ships-in-his-lifetime (accessed 2023-07-12).

[10] D. Heering, O. M. Maennel, and A. N. Venables, "Shortcomings in Cybersecurity Education for Seafarers," in *Proc. of MARTECH*, Lisbon, Portugal, 2020.

[11] Sjøfartsdirektoratet Norwegian Maritime Authority, "RSV 18-2022 - Reporting cyber incidents," Aug. 2022, Journal No. 2022/37521.

[12] M. Schwarz, M. Marx, and H. Federrath, "A structured analysis of information security incidents in the maritime sector," 2021, arXiv 2112.06545.

[13] Maritime Computer Emergency Response Team (M-CERT), "ADMIRAL," 2023. [Online]. Available: https://gitlab.com/m-cert/admiral

[14] "Marine Accident Report - Grounding of the U.S. Tankship EXXON VALDEZ on Bligh Reef, Prince William Sound, near Valdez, Alaska, March 24, 1989," National Transportation Safety Board, Washington, D.C., USA, Tech. Rep., 1990.

[15] T. M. Executive, "Panama Issues Report Critical of SCA Pilots in Ever Given Grounding," website, Jul. 2023. [Online]. Available: https://maritime-executive.com/article/panama-issues-report-critical-of-sca-pilots-in-ever-given-grounding