FORSCHUNG KOMPAKT

Maritimes Sicherheitslabor

Mehr IT-Sicherheit an Bord

Cyberattacken auf die Industrie und kritische Infrastrukturen nehmen weltweit zu. Auch Schiffe, die jedes Jahr Milliarden Tonnen Güter rund um den Globus transportieren, sind als Teil der globalen Lieferketten potenzielle Ziele – doch oftmals sind die IT-gestützten Bordsysteme nur schlecht gesichert. Um ein Bewusstsein für die Gefahren unzureichender Cybersicherheit auf See zu schaffen und Lösungen für die Abwehr von Cyberattacken zu entwickeln, baut die Forschungsgruppe »Maritime Cyber Security« am Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE zusammen mit dem Fraunhofer-Center für Maritime Logistik und Dienstleistungen CML ein modulares maritimes Sicherheitslabor auf, in dem Cyberangriffe auf Schiffe simuliert, erkannt und abgewehrt werden können.

Frühjahr 2021, Suezkanal: Das Frachtschiff »Ever Given« blockiert sechs Tage lang die Wasserstraße zwischen Rotem Meer und Mittelmeer, die eine wichtige Handelsroute unter anderem zwischen China und Europa darstellt. Ein einziger havarierter Frachter sorgt für einen langen Stau, in dem mehrere hundert Containerschiffe feststecken – mit Auswirkungen auf den Welthandel: Die Verzögerung führt unter anderem dazu, dass in den Häfen die Container knapp werden, Fahrpläne zum Teil noch für Monate durcheinandergeraten und Warenlieferungen verspätet eintreffen.

Der Vorfall zeigt, wie abhängig wir von maritimen Engpässen wie dem Suezkanal sind. Deutschland ist als Handelsnation auf einen reibungslos funktionierenden Im- und Export von Waren angewiesen: Dauert die Blockade einer wichtigen Handelsroute länger als ein paar Tage an, sind unmittelbare Störungen in der Produktion und Versorgung die Folge. Auch wenn der Grund für die Havarie im Fall der »Ever Given« nach Behördenangaben kein Cyberangriff war, ist gut vorstellbar, welche Auswirkungen eine erfolgreiche Attacke gegen die digitalen Navigations- und Kommunikationssysteme einzelner oder mehrerer Frachter haben könnte.

Schiffe als mögliche Angriffsziele

Insgesamt steigt für Schiffe der Bedarf an Vernetzung – sei es, um Routen ideal steuern zu können, Waren zu überwachen oder die Verbindung der Crew nach Hause zu ermöglichen. Damit werden maritime Systeme auch anfälliger für Cyberattacken. Grundsätzlich sind in diesem Kontext drei Angriffsarten vorstellbar, fasst Dr. Jan Bauer, Leiter

Kontakt
Roman Möhlmann | Fraunhofer-Gesellschaft, München | Kommunikation | Telefon +49 89 1205-1333 | presse@zv.fraunhofer.de
Silke Wiesemann | Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE | Telefon +49 228 9435-103 | Fraunhoferstraße 20 | 53343 Wachtberg | www.fkie.fraunhofer.de | silke.wiesemann@fkie.fraunhofer.de

der Forschungsgruppe Maritime Cybersicherheit am Fraunhofer FKIE, zusammen: »Allgemeine Angriffe sind nicht speziell gegen Schiffe gerichtet und aus diesem Grund die häufigste Bedrohung«, so Bauer. Ein mit Ransomware verseuchter USB-Stick, der in den Bordcomputer eingebracht wird, sei hierfür ein gutes Beispiel. »Weitaus gefährlicher sind gezielte Angriffe, die mit hohem Fachwissen durchgeführt werden und Schiffe zum Beispiel einfach vom Radar verschwinden lassen können«, betont er. Eine weitere Angriffsmöglichkeit liegt im sogenannten »Electronic warfare«, der zwar keinen Cyberangriff im engeren Sinne darstellt, aber ähnliche Auswirkungen haben kann, indem etwa die satellitengestützte Positionsbestimmung – zum Beispiel GPS – durch Störsender oder hochfrequente Radiowellen beeinflusst wird (»Jamming« oder »Spoofing«).

Realistische Testumgebung mit stationärer Schiffsbrücke

Diese unterschiedlichen cyber-physischen Angriffstypen – also Angriffe mit Auswirkungen auf die reale Welt – können die Forschenden des Fraunhofer FKIE in einem maritimen Sicherheitslabor simulieren. Aktuell wird die im Aufbau befindliche realitätsgetreue, stationäre Schiffsbrücke des CML in Hamburg im Rahmen des Projekts MaCy (Maritimes Cyber Security-Labor) zu einem Cybersicherheits-Labor erweitert. Die Umgebung stellt an Land alle Instrumente und Systeme bereit, die auch auf See zu finden sind – zum Beispiel die Brücken-Hardware, Seefunk- und AIS (Automatic Identification System)-Transceiver, ein Radargerät oder das ECDIS (Electronic Chart Display and Information System), das unter anderem für die Navigation genutzt wird. Innerhalb der realistischen und kontrollierten Testumgebung setzt die Forschungsgruppe unterschiedliche Entwicklungen ein, um IT-Sicherheitsvorfälle zu erkennen, zu untersuchen und bestenfalls abzuwehren.

Mit dem »Bridge Attack Tool« (BRAT) ist eine effektzentrierte Simulation möglich: Als Entwicklung aus dem Bereich der Offensive Security kann BRAT selbst unterschiedliche Angriffe – etwa Denial-of-Service (DOS)-Attacken oder Störungen und Manipulationen der Radar- und Positionierungssysteme – durchführen und deren konkrete Auswirkungen auf die Bordsysteme zeigen. So können die Forschenden nach der Auswertung beispielsweise Industriepartner auf bestehende Schwachstellen in Softwaresystemen hinweisen, sie bei der Nachbesserung unterstützen und Gegenmaßnahmen zum Beispiel aus dem Bereich der Kryptographie entwickeln.

Um Cyberangriffe an Bord möglichst frühzeitig abzuwehren, hat das Team ein maritimes »Intrusion detection system« entwickelt, das Anomalien automatisiert erkennt. Der »Cyber Incident Monitor« (CIM) wertet mögliche Angriffe aus und gibt über ein ergonomisches Benutzerinterface Hinweise und Handlungsempfehlungen an die Crew aus. »In Stresssituationen ist es wichtig, dass Warnmeldungen und Empfehlungen an das Schiffspersonal eindeutig und leicht umzusetzen sind«, so Florian Motz, Leiter der Forschungsgruppe »Organisationsergonomie« am Fraunhofer FKIE. »Daher haben wir bei CIM besonders darauf geachtet, dass akustische Warnsignale zum Beispiel erst dann

ausgelöst werden, wenn dringend gehandelt werden muss, und dass Warnmeldungen und Alarme mit Informationen und Entscheidungshilfen verbunden sind – etwa, dem GPS vorerst nicht mehr zu vertrauen. Das Konzept der Alarm- und Warnmeldungen ist an die Richtlinien der Internationalen Seeschifffahrts-Organisation (IMO) zum Brückenalarmmanagement angepasst.« Die Arbeiten an CIM und Teile der Weiterentwicklungen von BRAT wurden gemeinsam mit dem Unternehmen BM Bergmann Marine GmbH im Rahmen des Forschungsprojekts SINAV (Studie zur Integration und Verarbeitung von Sensorischen, Navigations-, Kommunikations- und Automationsinformationen für teil- und vollautonomen Betrieb von Schiffen zur Gewährleistung sicherer Navigation) für das Bundesministerium für Digitales und Verkehr durchgeführt.

Bewusstsein schaffen und Maßnahmen entwickeln

Mithilfe des innovativen maritimen Sicherheitslabors möchten die Forschenden bei Unternehmen, Behörden und Nautik-Fachleuten Bewusstsein für die Gefahren von Cyberattacken auf See schaffen und gemeinsam mit Partnern aus der Industrie Maßnahmen entwickeln. So können sie einerseits bestehende Systeme testen und nachrüsten, andererseits auch Untersuchungsdaten für die Entwicklung neuer Lösungen zur Verfügung stellen und so zur »Security by Design« beitragen: Konsequente Prävention in Kombination mit effektiven Methoden zur Detektion potenzieller Cyberangriffe sei der beste Schutz vor Schäden, meint Jan Bauer. »Wir dürfen uns nicht in falscher Sicherheit wiegen, nur weil Cyberangriffe auf Schiffe noch nicht in größerem Umfang bekannt geworden sind. Gerade auf älteren Frachtern, die schon seit Jahrzehnten in Betrieb sind, müssen die Systeme dringend nachgerüstet werden.« Die Motivation für ihre Arbeit haben die Forschenden klar vor Augen: Mit ihren Forschungsergebnissen möchten sie Angriffe erfolgreich verhindern und einen kleinen Baustein zur IT- und Cybersicherheit globaler Lieferketten beitragen – die wiederum essenziell für die geopolitische Sicherheit sind.

Abb. 1 Der Schiffsführungs-Simulator des Fraunhofer CML im Simulationsbetrieb im Hamburger Hafen.

© Fraunhofer CML

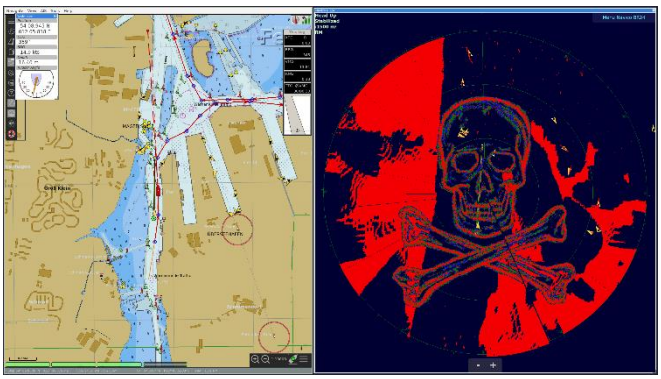

Abb. 2 Manipulation des Radarbilds durch das Bridge Attack Tool (BRAT) in einem Simulationsszenario in Rostock-Warnemünde.

© Fraunhofer FKIE