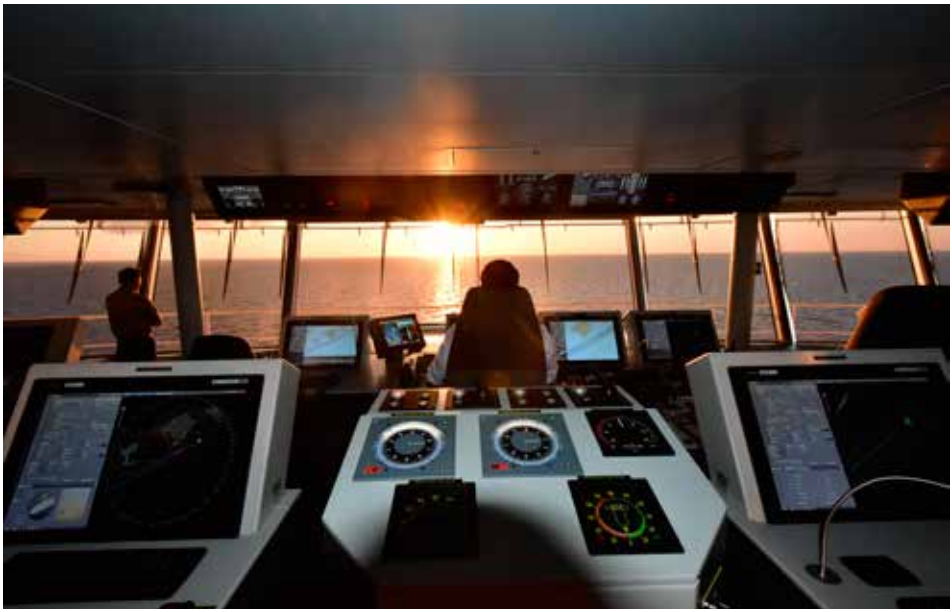

Auf der Brücke der „Nieuw Statendam“

Cybersecurity in der maritimen Wirtschaft

Vorschriften, aber auch das übergreifende unternehmerische Risikomanagement, erfordern heute eine gelebte Cybersecurity-Strategie.

Die Digitalisierung verändert Prozesse und Geschäftsmodelle quer über alle Branchen. Die maritime Wirtschaft befindet sich mitten in dieser Veränderung. Hochautomatisierte Terminals, intelligente Brückensysteme bis hin zu remote gesteuerten und teilweise bereits autonomen Fahrzeugen sind heute Realität.

Mit der steigenden Verbreitung digitaler Systeme und deren enger Vernetzung nimmt jedoch auch die Abhängigkeit von einer korrekt funktionierenden, hoch verfügbaren IT erheblich zu. Durch Fehlbedienung, insbesondere aber durch kriminelle Angriffe, können enorm hohe Schäden verursacht werden. Im Darknet erhältliche Schadsoftware macht es gleichzeitig einfach, einen kriminellen Angriff durchzuführen.

Ein beliebtes Einfallstor nicht nur in der maritimen Wirtschaft sind trickreich gestaltete E-Mails, die über zu öffnende Links oder Anhänge Schadsoftware installieren. Eine Variante dieser Schadsoftware sind Verschlüsselungstrojaner, die systematisch alle erreichbaren Daten verschlüsseln und die Zielorganisation zur Wiederherstellung der Daten erpressen. Bekannt wurde bereits 2017 der umfassende Systemausfall bei der dänischen Großreederei Maersk, bei dem 45.000 PC lahmgelegt wurden. Der Schaden betrug rund 300 Mio. USD. Eine andere Gruppe hat 2019 insbesondere Reedereien

aus Asien betrogen, indem über Schadsoftware Daten von Finanztransaktionen manipuliert wurden.

Ein anderes „Geschäftsmodell“ stand Pate bei dem Erpressungsversuch der australischen Werft Austal Shipyards, bekannt als Hersteller großer Katamaran-Schnellfähren. Es ging um vertrauliche Daten, die von den Erpressern kopiert wurden und deren Veröffentlichung angedroht wurde. Im September 2020 wurden Systeme der französische Großreederei CMA CGM mit einem Verschlüsselungstrojaner weltweit lahmgelegt.

Im Hafen von Antwerpen verschafften sich Drogenschmuggler durch Einschleusung von Schadenssoftware über einen USB-Stick Zugang zu Ladungspapieren, um gezielt Container mit Schmuggelware aus dem Hafen holen zu können.

Mehrfach wurde dokumentiert, dass GPS-Signale gestört wurden mit der Folge fehlerhafter Positionsangaben an Bord. Im Februar 2020 hat US-Präsident Trump daher für das Pentagon sowie weitere Behörden eine Minimierung der Abhängigkeit vom GPS-System angeordnet.

Das israelische Cybersecurity-Unternehmen Navaldome hat in mehreren Szenarien aufgezeigt, wie es die Kontrolle über zentrale Steuerungssysteme an Bord von Seeschiffen übernehmen konnte. Beispielsweise konnte das Unternehmen von außen und ohne Berechtigung die Rudermaschine steuern, das Ballastsystem kontrollieren sowie Positionsangaben auf der ECDIS-Seekarte und das Radarbild verfälschen.

Cyberangriffe sind somit bereits heute Realität, und das Schadenspotenzial ist gewaltig. Auf diese wachsende Bedrohung hat die IMO reagiert und die Sicherheitsregeln für den Schifffahrtsbetrieb (SOLAS) mit administrativen und technischen Mindestanforderungen an die Sicherheit von IT-Systemen ergänzt. Ab 1.1.2021 sind diese Vorschriften weltweit verpflichtend und Bestandteil der 5-jährigen Routineprüfungen sowohl des Document of Compliance (DoC) als auch der Klassenerteilung von Seeschiffen.

In Deutschland stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit dem IT-Grundschutz-Kompendium ein Rahmenwerk zur Verfügung, das in Zusammenarbeit mit dem Verein Hanseatischer Transportversicherer (VHT) und Consist zu Guidelines für den Land- und Schiffsbetrieb von Reedereien konkretisiert wurde. Die Umsetzung dieser neuen Anforderungen an die IT-Sicherheit erfordert Aufwand, sowohl an Bord als auch in den Reedereien an Land. Schon mit geringen Mitteln lässt sich die Sicherheit deutlich verbessern.

Zur Vermeidung von Problemen bei der Klasseerteilung und der Prüfung des DoC ist daher eine sorgfältige Vorbereitung erforderlich. Über die richtige Vorgehensweise informieren u. a. VHT, die Klassifizierungsgesellschaften und IT-Unternehmen mit entsprechender Kompetenz in Cybersecurity.

MARTIN LOCHTE-HOLTGREVEN

Martin Lochte-Holtgreven *ist seit 1995 Geschäftsführer der Consist Software Solutions GmbH. Nach Studienaufenthalten in Kiel und den USA war der Diplom-Mathematiker seit 1983 in der IT bei der Krupp MaK Maschinenbau GmbH tätig. Martin Lochte-Holtgreven wurde von 1993 bis 2003 als Sachverständiger für kommerzielle Datenverarbeitung öffentlich bestellt.*