SMART SHIPPING

Digital Safety First

| Digitalisierung | Seit diesem Jahr müssen Handelsschiffe ein Cybersecurity-Management nachweisen. Was dabei zu beachten ist und wie Reeder den neuen Anforderungen begegnen.

Text: Gunther Meyn

Schifffahrt war noch nie so sicher wie heute. Das gewährleisten schon die strengen Auflagen von IMO, Flaggenstaaten und Hafenbehörden: Zustand und Beschaffenheit von Schiff, Maschine und Ausrüstung werden in festen Abständen begutachtet, die Crews müssen regelmäßig Übungen für den Ernstfall absolvieren.

Das hohe Maß an Sicherheit in der maritimen Industrie ist unerlässlich. Schließlich geht es neben dem Transport hochwertiger Waren auch um die körperliche Unversehrtheit von Menschen auf hoher See. Doch neben den klassischen Gefahren ist die Schifffahrt vermehrt auch digitalen Bedrohungen ausgesetzt. Allein 2020 vermeldeten mehrere große Reedereien Cyberangriffe, darunter CMA CGM, MSC und Hurtigruten.

| Neue Disziplin | „Online-Kriminelle nutzen immer professionellere und effizientere Tools", so Jan Lausch, Cybersecurity-Experte bei Wärtsilä SAM Electronics. „Zudem steigt die Anzahl der Attacken und ihre Zerstörungskraft." An Einfallstoren an Bord der Schiffe mangelt es nicht: Ob Satellitenanlage, Router, Server, elektronisches Seekartensystem (ECDIS), Betriebssoftware oder Crew-Netzwerk – moderne Handelsschiffe sind heute vollgepackt mit IT. Auf Containerfrachtern der neuesten Generation funken zahlreiche Sensoren rund um die Uhr Betriebsdaten an die landseitigen IT-Zentralen. So lassen sich immer mehr Komponenten aus der Ferne warten und optimieren. Das macht die Systeme aber auch anfälliger für Cyberattacken. Entsprechend wichtig ist ein gut organisiertes und dokumentiertes Cyber-Safety-Management. Bislang galten dafür keine Auflagen. Doch seit Januar 2021 müssen Schiffe einen entsprechenden Nachweis erbringen. Das schreibt die 2017 erlassene IMO Resolution MSC 428 (98) vor.

„Cybersecurity-Checks werden künftig im Rahmen der Port State-Control durchgeführt", sagt Martin Lochte-Holtgreven,

Fotos: Consist Software Solutions, todor – stock.adobe.com

Netzsicherheit. Die Schiffs-IT auf modernen Frachtern wird immer komplexer. Das erfordert effiziente Schutzmaßnahmen.

Geschäftsführer von Consist Software Solutions. „Wer hier durchfällt, muss zumindest mit einer Mängelrüge rechnen." Sein Unternehmen bietet regelmäßig Quick Checks und Pre-Audits an, bei denen IT-Experten stichprobenartig prüfen, wie gut Reedereien und Shipmanager in Sachen Cybersicherheit (CS) aufgestellt sind. „Vor allem bei kleineren Betrieben besteht hier mitunter noch erheblicher Nachholbedarf", so Lochte-Holtgreven.

| Risikofaktor Mensch | Die Zeit drängt. Schiffsbetreiber sollten spätestens bis zum nächsten anstehenden ISM-Audittermin ihre Hausaufgaben machen. Der erste Schritt ist immer eine sorgfältige Risikoanalyse und Dokumentation der gesamten Bord-IT. Welche Systeme und Hardwarekomponenten sind installiert? Wie hoch ist der Vernetzungsgrad? Besteht ausreichend Schutz durch Firewalls und Anti-Malware-Programme? Wie bzw. wie oft werden Software-Updates und Sicherheits-Back-ups durchgeführt?

Ob Virus, Malware oder Erpressungsversuche mittels Ransomware-Attacken – die potenziellen Gefahren von außen sind bekannt und gefürchtet. Als größtes Einfallstor gilt ein unkontrollierter Datenverkehr. „Ein nicht autorisierter USB-Stick ist hochriskant", warnt Lochte-Holtgreven. Problematisch ist auch die sogenannte „Schatten-IT". So bezeichnet man die nicht autorisierte Installation oder Manipulation von Hard- und Software durch Mitarbeiter. „Da hat dann ein Crewmitglied einfach mal das Netzwerkkabel umgestöpselt oder gleich seinen eigenen Router angeschlossen, um schneller ins Internet zu kommen", so Experte Lochte-Holtgreven.

Das oberste Gebot lautet deshalb: Crew-IT und Betriebs-IT strikt voneinander trennen! Außerdem gilt: autorisierte Personen benennen und den Crewmitgliedern einen verantwortungsvollen Umgang mit der Bord-IT einschärfen. „Awareness" nennt man das im Fachjargon. Ein Begriff, der regelmäßig auf den To-do-Listen und Cybersecurity-Guidelines von BIMCO, Flaggenstaaten und Klassifikationsgesellschaften zu finden ist.

Auch ein Krisenmanagement gehört ins CS-Pflichtenheft. Wie reagiert die Besatzung auf einen IT-Angriff? Gibt es für diese Fälle klare Anweisungen? Wer hat die nötige Kompetenz, um zu reagieren? All das muss für die künftigen Reviews sorgfältig dokumentiert werden – sowohl für die eigene Flotte als auch für gecharterte Schiffe. Besonders penible Kontrollgänge drohen durch die US-Küstenwoche. Laut Svante Einarsson, Team Leader Cyber Security bei DNV GL, achten die Auditoren nicht nur auf unbefugte USB-Sticks, sondern überprüfen auch die Bord-Software und fahnden nach Sicherheitslücken.

| Hürden genommen | Die meisten deutschen Reeder sind laut Einarsson in Sachen CS-Compliance gut aufgestellt. Dazu gehört auch Auerbach Schifffahrt. Bei dem Hamburger Unternehmen hat man bereits vor anderthalb Jahren einen internen Experten mit der Einführung eines regelkonformen CS-Managements beauftragt. Zum umfangreichen Maßnahmenpaket gehörte unter anderem die Deaktivierung von USB-Ports, und ein Sicherheits-Recovery-Update auf virtuellen Rechnern sowie die Implementierung einer neuen Softwarelösung.

Die Umstellung auf das neue Regelwerk war nicht immer problemlos, denn das Durchschnittsalter von Auerbachs Multipurpose-Flotte liegt bei zwölf Jahren. „Bei unseren älteren Schiffen erwies sich die IT-Aufrüstung als echte Herausforderung", erinnert sich Auerbachs IT-Manager Tobias Landwehr. Auch er weiß: Alle Sicherheitsregeln fruchten nur, wenn die Crew mitzieht. Er vergleicht die Akzeptanz mit der Gurtpflicht fürs Auto: „Die wurde auch erst langsam angenommen."

Cybersecurity ist ein fortlaufender Prozess und muss konstant weiterentwickelt werden – schließlich lassen sich die Angreifer immer raffiniertere Methoden einfallen. Landwehr wünscht sich hier mehr Kooperation zwischen den Reedereien. „Wir sollten uns regelmäßig über Vorfälle austauschen und zusammenarbeiten – denn das macht die Gegenseite auch!" |•••

Experte. Martin Lochte-Holtgreven, Geschäftsführer Consist Software Solutions, berät Reedereien.