360.000 Cyber-Angriffe jeden Tag

Täglich werden inzwischen 360.000 Cyberangriffe weltweit gemeldet. Allein im vergangenen Jahr gab es einen Anstieg um knapp 40%. Der Schaden, den kriminelle Hacker anrichten, wird auf 2 Bio. $ jährlich geschätzt – Tendenz steigend.
Von *Krischan Förster*

Die Bedrohung durch Cyber-Kriminalität ist auch in der Schifffahrt in aller Munde, spätestens nachdem 2017 das NotPetya-Virus über Tage Terminals und Schiffe des weltgrößten Reedereikonzerns Maersk lahm gelegt hat. Den Schaden bezifferten die Dänen damals mit rund 350 Mio. $.

Für den CEO des IT-Unternehmens Cisco, Chuck Robbins, steht daher fest: »Es gibt heute zwei Arten von Unternehmen. Die, die schon gehackt wurden, und solche, die noch nicht wissen, dass sie gehackt wurden.«

Anlass genug für das Maritime Cluster Norddeutschland (MCN), dieses Thema auf einer Veranstaltung unter der Überschrift »Cyber Security an Bord – quo vadis?« zu diskutieren. Das Ziel: »Wir wollen die Möglichkeit geben, voneinander zu lernen«, sagte Andreas Born, Leiter der Bremer MCN-Geschäftsstelle, bei der Begrüßung der rund 120 Teilnehmer im Internationalen Maritimen Museum Hamburg.

»Schutzgelderpressung wieder da«

Cyberkriminalität sei heute ein Millionengeschäft mit vergleichsweise wenig Aufwand und geringem Entdeckungsrisiko für die Täter, sagt Thorben Lorenzen vom Sicherheitsdienstleister Securepoint. »Das Zeitalter der Schutzgelderpressung ist wieder da«. Das Handwerkszeug für einen Cyberangriff sei im Darknet für wenig Geld oder gegen Gewinnbeteiligung zu kaufen, berichtete der Experte.

Der durchschnittliche Schaden, der durch Lösegeldforderungen, Betriebsausfälle oder -störungen entstehe, liegt mittlerweile bei etwa 4 Mio. $ pro Fall. Und es könne jeden treffen, jederzeit. Es gebe zwar keinen hundertprozentigen Schutz, doch müssten Unternehmen verstärkt Vorkehrungen treffen, um sich gegen die Angriffe aus dem weltweiten Netz zu wappnen –sowohl gegen die klassischen IT-Lösungen (Netz, E-Mail etc.) als auch gegen die Operation Technology (OT) wie kommerzielle Anwendungen an Land und an Bord.

Sowohl technisch, organisatorisch als auch konzeptionell wird in der Schifffahrt jedoch derzeit eher noch »Pionierarbeit« geleistet. Verbindliche Richtlinien der IMO, die in den Safety Management Systemen der Reedereien umgesetzt werden müssen, treten erst ab 2021 in Kraft.

Einstweilen gibt es Handlungsempfehlungen verschiedener Institutionen wie BIMCO, Intertanko, DNV GL oder auch vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI). Zum Teil gelten diese allerdings nur für den Landbetrieb, nicht aber für den Schiffsbetrieb. Auch Haftungs- und Versicherungsfragen sind vielfach noch ungeklärt.

> *»Es gibt heute zwei Arten von Unternehmen. Die, die schon gehackt wurden, und solche, die noch nicht wissen, dass sie gehackt wurden«*
>
> Chuck Robbins, CEO Cisco

Neue Policen speziell für die Deckung von Cyber-Crime-Risiken, wie sie der Bremer Assekuradeur Lampe & Schwartze seit dem vergangenen Jahr anbietet, sind die Ausnahme. »Reeder müssen anerkennen, dass Cyber-Angriffe ein weltweites Phänomen sind, das auch die Technologie des Schiffes beeinträchtigen und zu schweren finanziellen und Reputationsverlusten führen kann«, sagt Christoph Enge, geschäftsführender Gesellschafter bei Lampe & Schwartze.

Erheblicher Aufwand

»Für uns steht ganz klar im Vordergrund, wie wir im Falle eines Angriffs ohne Unterbrechung weiterarbeiten können«, sagte Lars Bremer, Geschäftsführer der Bremer Tanker-Reederei Carl Büttner. Gerade mittelständische Unternehmen müssten erheblichen personellen und finanziellen Aufwand betreiben, um die Sicherheit ihrer Netzwerke zu erhöhen. Büttner versucht dies, mit virtuellen Netzwerken zu lösen, die einander bei einem Angriff ersetzen können.

Bei Auerbach Schifffahrt aus Hamburg wird gerade die gesamte IT-Ausstattung an Land und an Bord der derzeit 14 Schiffe neu aufgesetzt. »Es gibt keinen ›Königsweg‹, keine beste Lösung«, sagt Tobias Landwehr, IT Project Manager der MPP-Reederei. Aber es gehe darum, die Netzwerke möglichst robust zu machen und keine Einfallstore für Cyberkriminelle offen zu lassen.

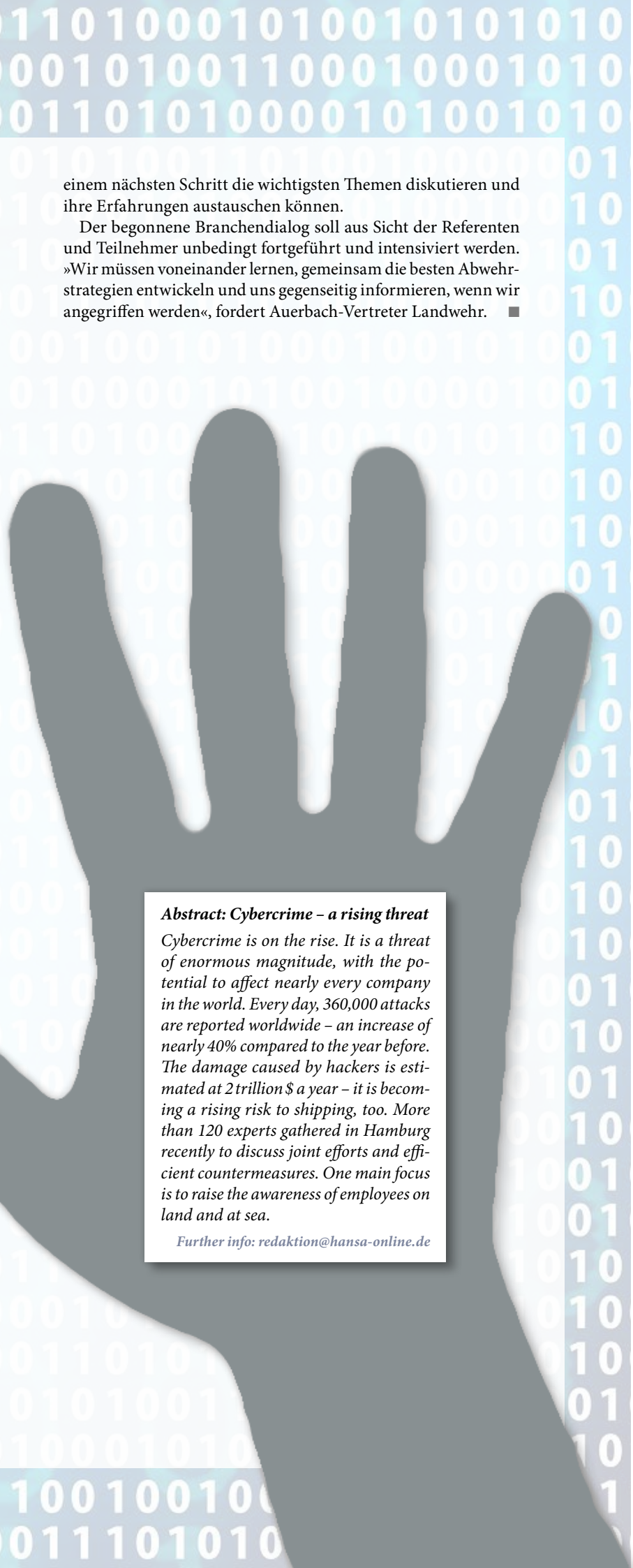
Wichtigster Punkt bei allen Bemühungen sei die Schulung der Mitarbeiter. Unwissenheit und Fahrlässigkeit verursachen derzeit jeden zweiten Schadensfall. »Darauf müssen wir das größte Augenmerk legen«, sagt Frank Jungmann, Geschäftsführer von German Tanker Shipping. Die Reedereien sind nach eigenen Angaben dabei, alle Erkenntnisse und Anforderungen in einer Art IT-Grundsatz-Katalog mit klaren Handlungsempfehlungen für die Mannschaften an Land und auf den Schiffen zu sammeln.

Austausch unter Gleichgesinnten

Hier nun kommt das MCN als Branchennetzwerk ins Spiel. Das Fachforum in Hamburg mit der HANSA als exklusivem Medienpartner hat die Akteure aus der Schifffahrt erstmals zusammengebracht. In sogenannten »geschützten Projekträumen« sollen sie in

einem nächsten Schritt die wichtigsten Themen diskutieren und ihre Erfahrungen austauschen können.

Der begonnene Branchendialog soll aus Sicht der Referenten und Teilnehmer unbedingt fortgeführt und intensiviert werden. »Wir müssen voneinander lernen, gemeinsam die besten Abwehrstrategien entwickeln und uns gegenseitig informieren, wenn wir angegriffen werden«, fordert Auerbach-Vertreter Landwehr. ■



Abstract: Cybercrime – a rising threat

Cybercrime is on the rise. It is a threat of enormous magnitude, with the potential to affect nearly every company in the world. Every day, 360,000 attacks are reported worldwide – an increase of nearly 40% compared to the year before. The damage caused by hackers is estimated at 2 trillion $ a year – it is becoming a rising risk to shipping, too. More than 120 experts gathered in Hamburg recently to discuss joint efforts and efficient countermeasures. One main focus is to raise the awareness of employees on land and at sea.

Further info: redaktion@hansa-online.de

LAMPE & SCHWARTZE

Cyber-Police bietet Reedern speziellen Schutz

Ab sofort bietet der Bremer Assekuradeur Lampe & Schwartze eine Cyberpolice für Reeder, die von großen Versicherern wie der Allianz und Ergo gedeckt wird. »Mit der zunehmenden Digitalisierung steigen auch die Cyberrisiken – Schiffe werden immer anfälliger«, sagt Arne Linke, Abteilungsleiter Schiffsversicherungen bei der Ergo.

Reedereien können sich nun auch im deutschen Markt gegen Sachschäden an Schiff und Maschine durch Cyberattacken versichern. »Wir haben ein solides Wording entwickelt, relevante Kapazitäten beschafft und auch ein Dienstleisternetzwerk aufgebaut. Bisher waren solche Lösungen nur im Ausland verfügbar, beispielsweise in Norwegen«, sagt der geschäftsführende Gesellschafter von L&S MU, Hans-Christoph Enge. Die Cyber-Police deckt folgende Risiken ab:

- Kaskoschäden, die als Folge eines Cyberangriffs auf das Schiff entstehen,
- Krisenmanagementkosten für den Einsatz von IT-Experten zum Erkennen und Abwehren eines Cyberangriffs,
- Kosten für die Wiederherstellung betroffener Schiffssysteme.

Lampe & Schwartze hatte bereits vor einem Jahr eine eigene Zusatzpolice unter dem Namen »Ship Owner's Marine Cyber Cover« auf den Markt gebracht. Nun sind auch große Versicherer mit an Bord, um die Risikokapazitäten zu erweitern.

Bei diesem Deckungskonzept handle es sich um ein Ergänzungsprodukt zu bereits bestehenden Kaskopolicen wie der klassischen Seekaskoversicherung. »Ein Cyberangriff auf das Navigationssystem eines Schiffes oder Steuerungssysteme kann schlimmstenfalls zu einer Kollision oder Strandung führen«, sagt Justus Heinrich, der beim Spezialversicherer Allianz Global Corporate & Specialty (AGCS) für die Schiffsversicherung verantwortlich ist. Laut des »Safety und Shipping Review 2019« der AGCS sind Cyber-Vorfälle das zweitgrößte Risiko für die Schifffahrt nach Naturkatastrophen und Elementargefahren.

Die neue Cyber-Deckungserweiterung bietet neben der Absicherung von Sachschäden durch einen Cyber-Vorfall auch diverse Service-Leistungen durch hochspezialisierte Dienstleister. So steht im Schadensfall der Verein Hanseatischer Transportversicherer (VHT) für Schadensbearbeitung und Risikoanalyse sowie das Maritime Cyber Emergency Response Team (MCERT) in Großbritannien als Berater und Forensiker zur Verfügung. ■