Foto: Lochte-Holtgreven

Moderne Schiffe werden als schwimmende Rechenzentren immer häufiger zum Ziel von Cyberpiraten.

Cyberpiraten im Aufwind

Wie Abwehrkonzepte für See- und Binnenschifffahrt aussehen können, erfuhr PROTECTOR von Martin Lochte-Holtgreven, Geschäftsführer der Consist Software Solutions GmbH.

ANNABELLE SCHOTT-LUNG

Bereits in einem James-Bond-Film von 1997 wurde ein Schiff gehackt – damals reine Science Fiction?

» Martin Lochte-Holtgreven: Lassen Sie uns zunächst den Begriff „Hacking" klären. Wenn wir darunter die Verschaffung eines Zugangs zu einem Computersystem durch Unberechtigte verstehen, so gibt es Hacking seit der Einführung von Zugriffskontrollsystemen auf Computern, und natürlich auch auf Schiffen. 1997 war jedoch die Vernetzung von Computern, und insbesondere die an Bord der kommerziellen Schifffahrt, noch sehr gering, und damit war das Eindringen in Rechnersysteme von „remote" tatsächlich noch Science-Fiction in Bezug auf die maritime Wirtschaft.

20 Jahre später traf es die Reederei Maersk. Die komplette IT wurde durch einen Ransomware-Angriff lahmgelegt. Hat man bis dahin die Gefahr von Cyberangriffen unterschätzt?

» Martin Lochte-Holtgreven: Nach meinem Eindruck hat man gerade in größeren Unternehmen schon seit vielen Jahren die Bedrohung durch Cyberangriffe durchaus ernst genommen.

Die Erfahrungen aus realen Vorfällen haben dann gezeigt, dass man wegen der Schnelligkeit, mit der sich Schadsoftware in Computernetzen verbreiten kann, auch sehr schnell wirksame Notfallmaßnahmen benötigt.

In dem gennanten Beispiel von Maersk breitete sich der Notpetya-Virus im Unternehmensnetz innerhalb weniger Minuten weltweit aus. Es bedarf also eines ständigen Monitorings und sehr schneller Response-Prozesse, um bei einem Eindringen ins Netz zu versuchen, wenigstens Teile des eigenen Netzwerks vor der Schadsoftware zu schützen.

Foto: Consist Software Solutions GmbH

„Es gilt, durch entsprechende Schulung die Awareness auf den Umgang mit Passwörtern und Mails an Bord auszuweiten."

Martin Lochte-Holtgreven,
Geschäftsführer der Consist Software Solutions GmbH

Beim Grad ihrer Digitalisierung und mit den Werten, die sie transportieren, sind Schiffe ideale Ziele für Cyberpiraten …

» Martin Lochte-Holtgreven: Ja, diese Gefahren sind real. In der Praxis zeigt es sich bislang, dass die Angreifer sich eher auf zentrale Systeme konzentrieren und weniger auf individuelle Schiffe mit ihren individuellen IT-Netz- und Kommunikationskomponenten. Es hängt dabei von den Absichten der Angreifer ab. Geht es um Erpressung, Ladungsinformationen für einen Raubüberfall auf eine ganz genau bestimmte Fracht oder die Störung von Betriebsabläufen?

Wie viele Cyberangriffe auf Reedereien oder Schiffe gibt es jährlich? Werden solche Angriffe überhaupt erkannt?

» Martin Lochte-Holtgreven: Wirklich aussagefähige Zahlen zu Cyberangriffen gibt es nicht. Nicht alle Angriffe werden erkannt, viele werden nicht öffentlich, und schließlich ist auch die Zählweise schwierig festzulegen. Wenn bei einem Brute-Force-Angriff maschinell Passworte ausprobiert werden, ist dann jeder Versuch ein einzelner Angriff? Daher sind Aussagen wie die vom Port of Los Angeles gemeldeten 40 Millionen Cyberangriffe pro Monat schwer zu bewerten. Lassen Sie es mich so sagen: Wir wissen es nicht wirklich genau, aber das ist auch nicht wichtig. Wichtig ist zu erkennen, dass es sie gibt und sie jederzeit jede Organisation und jedes Netzwerk treffen können.

Jetzt ist IT-Sicherheit ja schon an Land ein Problem, aber auf dem Wasser …? Kann eine Schiffs-IT überhaupt homogen sein?

» Martin Lochte-Holtgreven: Die technische Ausstattung an Bord ist naturgemäß heterogen, und das gilt auch für die IT-Komponenten. Mit der Zeit wird die Konfiguration an Bord meist noch viel stärker verändert, zum Beispiel durch den Ersatz defekter Komponenten in abseits gelegenen Fahrtgebieten. Eine noch größere Schwachstelle entsteht durch mangelnde Systemwartung. Die Installation aktueller Versionen von Betriebssystemen und Software, insbesondere aber die Einspielung von Sicherheitspatches, sind im Schiffsbetrieb nur schwer zeitnah zu leisten und führen zu einer höheren Verwundbarkeit.

Die geführte Flagge impliziert auch die Gültigkeit der jeweiligen nationalen Gesetze an Bord. Eine höhere praktische Bedeutung haben heute jedoch die Regelungen der IMO (International Maritime Organization – die für Schifffahrt und Seeverkehr zuständige Unterorganisation der UN) sowie die sich in einer starken Entwicklung befindlichen Anforderungen der Klassifizierungsgesellschaften, die mit eigenen „Cybersecure"-Einstufungen die Vorkehrungen gegen Cyberangriffe an Bord bewerten und somit den Versicherungsgesellschaften als Maßstab dienen.

Seit dem 1. Januar 2021 müssen Unternehmen den IMO-Richtlinien für das maritime Cyber-Risikomanagement zufolge Risiken in ihren bestehenden Sicherheitssystemen angemessen berücksichtigen. Wurde das seitdem umgesetzt?

» Martin Lochte-Holtgreven: Die IMO-Anforderung besagt, dass seit dem 1.1.2021 für jedes Seeschiff bei der alle fünf Jahre fälligen großen Untersuchung („Klasseprüfung") ein IT-Sicherheitskonzept vorgelegt werden muss. Inwieweit dies wirklich geprüft wird, da gibt es berechtigte Zweifel. Jedenfalls liegt das Know-how der traditionellen Klasse-Prüfer eher im Maschinenbau als in der IT-Welt, und es ist zu vermuten, dass die Auditierung der IT-Sicherheit an Bord aktuell oftmals nicht ausreichend erfolgt. Das wird sich aber im Laufe der Zeit ändern, denn auch die Klassegesellschaften lernen diesbezüglich deutlich dazu und erweitern ihr Know-how. Ich gehe also davon aus, dass nach und nach tatsächlich die Umsetzung nachprüfbar erfolgt.

Was besagt das IT-Grundschutz-Profil „Schiffsbetrieb", das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt wurde?

» Martin Lochte-Holtgreven: Das vom BSI entwickelte Grundschutz-Profil geht über die Anforderungen der IMO hinaus und gibt erheblich konkretere Hinweise zur Detaillierung und Umsetzung eines IT-Sicherheitskonzeptes an Bord. Allerdings liegen die aktuellen Schwachpunkte an Bord meist in so elementaren Bereichen wie dem physischen Zugang zu Servern, fehlenden Updates grundlegender Systeme oder dem fahrlässigen Umgang mit Passwörtern und Mails. Hier gilt es zunächst anzusetzen!

Gibt es „Security by Design" schon in der Planungsphase eines Schiffes?

» Martin Lochte-Holtgreven: Diese Überlegungen ziehen langsam in die Planungen ein und folgen damit den physischen Vorkehrungen wie der Einrichtung einer Zitadelle, eines gehärteten Schutzraums. Für die IT geben dabei die Anforderungen der Klassegesellschaften wichtige Leitlinien.

Es bleibt aber die „Schwachstelle" Mensch – auch oder gerade auf einem Schiff. Dort wird gearbeitet und gelebt, die Seeleuten sind aus den unterschiedlichsten Ländern und Kulturkreisen. Wie schafft man hier ein Grundverständnis für das Thema Cybersicherheit?

» Martin Lochte-Holtgreven: Schulung, Schulung, Schulung. Immerhin nimmt die Affinität zur IT insgesamt zu, und das Wissen zum Beispiel um den vorsichtigen Umgang mit Social Media ist weltweit ein Thema – insbesondere bei Menschen, die bereits in ihren Herkunftsländern den vorsichtigen Umgang mit freien Meinungsäußerungen gelernt haben. Es gilt, durch entsprechende Schulung diese Awareness auf den Umgang mit Passwörtern und Mails an Bord auszuweiten.

Wie wird der Notfall auf einem Schiff geprobt? Gibt es Penetrationstests?

» Martin Lochte-Holtgreven: Die Übung zu einem Ausfall von IT-Systemen an Bord ist noch nicht Routine, sondern Ausnahme. Und ja, es gibt schon Überprüfungen der Netzwerk-Sicherheit auch durch simulierte Angriffe, allerdings auch mit ernüchternden Ergebnissen – ein Verfahren, das einige Anbieter von Security-Lösungen gern nutzen, natürlich in Abstimmung mit den potenziellen Kunden. ■

Consist Software Solutions GmbH:
www.consist.de