21.09.2021

Maritime Cyber Security

- Vorbereitung auf den (Cyber-)Notfall
- Effektives Cyber-Risk-Management notwendig
- Deutsche Flagge unterstützt Reedereien
- FAQs

Vorbereitung auf den (Cyber-)Notfall Auch für die Seeschifffahrt als wichtiger Teil der Logistikkette wird das Thema Cyber-Sicherheit immer wichtiger. Spätestens der Angriff mit der Schadsoftware "NotPetya" im Jahr 2017, bei dem allein bei der Maersk-Reederei ein Schaden von mehreren hundert Millionen Euro entstand, hat deutlich gemacht, welche immensen Ausmaße Cyber-Angriffe in der Seeschifffahrt haben können. Solche Angriffe zum Beispiel auf die elektronischen Navigationssysteme oder den Hauptantrieb an Bord könnten sogar zu Totalverlusten von Schiffen führen.

Die internationale Seeschifffahrtsorganisation IMO hat die Bedeutung des Themas Cyber Security erkannt und fordert die Reedereien auf, sich vor Cyber-Risiken zu schützen (IMO Resolution MSC.428(98)). Die Schiffsbetreiber müssen wirksame Maßnahmen zum Schutz gegen Cyber-Angriffe erarbeiten und in ihre bestehenden ISM-Systeme integrieren.

Effektives Cyber-Risk-Management notwendig Wie können sich Reedereien effektiv vor Cyber-Angriffen schützen? Indem sie zunächst mögliche Cyber-Risiken identifizieren, analysieren und bewerten, um dann konkrete Maßnahmen zur Reduzierung dieser Risiken an Bord und an Land zu ergreifen. Ziel dieses Cyber-Risk-Managements ist es, den Schiffsbetrieb widerstandsfähiger zu machen und umfassend vor Cyber-Angriffen zu schützen.

In der Praxis hat sich für Reedereien das Vier-Stufen-Modell für das Cyber-Risk-Management bewährt:

- Prüfe
Welche Cyber-Risiken bringt mein Schiffsbetrieb mit sich?

- Bewerte
Sind meine derzeitigen Maßnahmen ausreichend oder sind weitere Maßnahmen notwendig?

- Setze um
Geeignete weitere technische, organisatorische, persönliche Maßnahmen festlegen und umsetzen.

- Analysiere
Maßnahmen zur Reduzierung und Vermeidung von Cyber-Risiken regelmäßig einer Wirksamkeitskontrolle zu unterziehen

Reedereien müssen spätestens ab dem ersten ISM-Office-Audit nach dem 1. Januar 2021 gegenüber ihrer Flaggenstaatverwaltung nachweisen, dass sie Cyber-Risiken bewertet und geeignete Sicherheitsmaßnahmen umgesetzt haben.

(nach oben)

Deutsche Flagge unterstützt Reedereien Die deutsche Flaggenstaatverwaltung unterstützt die Reedereien, ein ganzheitliches Cyber-Risiko-Management an Land und an Bord ihrer deutschflaggigen Schiffe zu entwickeln. Die BG Verkehr, das BSH und das Bundesamt für Sicherheit in der Informationstechnik (BSI) geben in ihrem Rundschreiben "ISM Cyber Security" praktische Tipps zum Thema Cyber-Sicherheit. Als Mindestabsicherung empfehlen sie die sogenannten IT-Grundschutzprofile des BSI zum Landbetrieb und zum Schiffsbetrieb. Diese Muster-Sicherheitskonzepte enthalten konkrete Empfehlungen für IT-Sicherheitsmaßnahmen an Bord und an Land.

(nach oben)

FAQ Maritime Cyber Security

Müssen Reedereien Cyber-Risk-Unterlagen zur Prüfung bei der BG Verkehr einreichen?

Nein, die Umsetzung des Cyber Risk Managements in einer Reederei wird im Rahmen der externen ISM-Audits abgeprüft.

Was bedeuten die beiden Begriffe "IT" und "OT"?

Der Begriff "IT" umfasst Informationstechnologie und Netzwerke an Bord wie z. B. Computer, Server, WLAN, Internet, Telefon.

Der Begriff "OT" (Operational Technology) bezieht sich auf Systemanlagen an Bord wie z. B. Radar, ECDIS, GNSS, Maschinensteuerung, Sensoren und Alarme.

Muss der interne Auditor des Unternehmens ein IT-Spezialist sein?

Nein, der interne Auditor des Unternehmens prüft die Umsetzung des Safety Management System (SMS) und nicht die Funktionalität von IT- und OT-Systemen.

Müssen Reedereien für den Cyber-Schutz ein eigenes ISO-Managementsystem einführen?

Nein, ein eigenständiges Cyber-Managementsystem (wie z. B. ISO 27000) ist nicht zwingend erforderlich. Die Umsetzung innerhalb des Safety Management System (SMS) der Reederei ist ausreichend. Reedereien können sich aber auf Grund der Art und Größe ihres Unternehmens entscheiden, eine separate Zertifizierung wie ISO 27000 einzuführen. Sie erfüllen damit die Vorgaben der IMO zum Cyber Risk Management (IMO Resolution MSC.428(98)), wenn das zertifizierte System in das Safety Management System der Reederei eingebunden wird.

Welche Mindestinhalte gehören zu einem Cyber-Notfallplan?

Zu einem Cyber-Notfallplan gehören:

- Aufgaben, die ab dem Zeitpunkt des Erkennens eines Vorfalls einzuleiten sind (Reagieren auf Cyber-Vorfälle und deren Folgen - keine präventiven Aufgaben),
- Maßnahmen zum Wiederherstellen (Backup & Restore),
- Notfallrufnummern und
- Meldeketten einschließlich Notfallteam "Land".