(VkBl. 23/184/16)

Nr. 184 **Bekanntmachung des IMO-Rundschreibens MSC.1/Circ.1526 vom 01. Juni 2015**

Hiermit wird das nachstehende Rundschreiben MSC.1/Circ.1526 (vom 01. Juni 2015) „INTERIMSRICHTLINIEN FÜR MARITIMES CYBER-RISIKOMANAGEMENT“ der Internationalen Seeschifffahrts-Organisation (International Maritime Organisation (IMO)) in deutscher Sprache amtlich bekannt gemacht.

Hamburg, den 04.10.2016

Bundesamt für
Seeschifffahrt und Hydrographie
Monika Breuch-Moritz
Präsidentin

Interimsrichtlinien für maritimes Cyber-Risikomanagement

1 Der Schiffssicherheitsausschuss hat in seiner sechsundneunzigsten Sitzung (11.–20. Mai 2016) die im Anhang aufgeführten *Interimsrichtlinien für maritimes Cyber-Risikomanagement* verabschiedet, nachdem er den dringenden Bedarf, auf Cyber-Bedrohungen und -Schwachstellen aufmerksam zu machen, festgestellt hatte.

2 Die Richtlinien beinhalten allgemeine Empfehlungen für das maritime Cyber-Risikomanagement, um die Seeschifffahrt vor derzeitigen und aufkommenden Cyber-Bedrohungen und -Schwachstellen zu schützen. Die Richtlinien enthalten außerdem funktionale Elemente, die das effektive Cyber-Risikomanagement unterstützen.

3 Die Mitgliedsregierungen werden hiermit aufgefordert, dieses Rundschreiben allen Betroffenen zur Kenntnis zu bringen.

Anhang

Interimsrichtlinien für maritimes Cyber-Risikomanagement

1 Einführung

1.1 Diese Richtlinien beinhalten allgemeine Empfehlungen für das maritime Cyber-Risikomanagement. Für die Zwecke dieser Richtlinien bezieht sich das maritime Cyber-Risiko auf das Ausmaß, in dem ein Technologiebestandteil durch einen potenziellen Umstand oder ein Ereignis bedroht ist, das zu schifffahrtsbedingten, betrieblichen Schutz- oder Sicherheitsversagen infolge beschädigter, verlorener oder gefälschter Informationen oder Systeme führen kann.

1.2 Die Interessenvertreter sollten die erforderlichen Schritte unternehmen, um die Schifffahrt vor aktuellen und in Entstehung befindlichen Bedrohungen und Schwachstellen in Verbindung mit der Digitalisierung, Integration und Automatisierung von Prozessen und Systemen in der Schifffahrt zu schützen.

1.3 Für Einzelheiten und Anleitung bezüglich der Entwicklung und Implementierung spezifischer Risikomanagementprozesse sollten die Nutzer dieser Richtlinien die jeweiligen Anforderungen der Mitgliedsstaaten und Flaggenstaatsverwaltungen zu Rate ziehen sowie die einschlägigen internationalen und Industriestandards und bewährte Verfahren.

1.4 Das Risikomanagement ist wesentlich, um den Schiffsbetrieb zu schützen und zu sichern. Das Risikomanagement hat sich traditionell auf Vorgänge im physikalischen Bereich beschränkt, jedoch hat der zunehmende Rückgriff auf die Digitalisierung, Integration und Automatisierung netzwerkbasierter Systeme in der Schifffahrtsbranche zu einem wachsenden Bedarf an Cyber-Risikomanagement geführt.

1.5 Ausgerichtet auf das Ziel, den Schutz und die Sicherheit der Schifffahrt zu unterstützen, die gegenüber Cyber-Risiken betrieblich belastbar ist, stellen diese Richtlinien Empfehlungen zur Verfügung, die in die vorhandenen Risikomanagementprozesse integriert werden können. In dieser Hinsicht stellen die Richtlinien eine Ergänzung der Managementpraktiken zur Sicherheit und Gefahrenabwehr dar, die von dieser Organisation eingerichtet wurden.

2 Allgemein

2.1 Hintergrund

2.1.1 Cyber-Technologien sind für den Betrieb und das Management zahlreicher Systeme unerlässlich geworden, die für die Sicherheit und die Gefahrenabwehr in der Schifffahrt und den Schutz der Meeresumwelt entscheidend sind. In einigen Fällen müssen diese Systeme internationale Standards einhalten und mit Anforderungen der Flaggenstaatsverwaltung übereinstimmen. Die Schwachstellen, die durch den Zugriff, das Verbinden oder Vernetzen dieser Systeme erzeugt werden, können zu Cyber-Risiken führen, mit denen man sich befassen sollte. Verletzbare Systeme können folgendes beinhalten, ohne darauf beschränkt zu sein:

- Brückensysteme;
- Ladungsbehandlungs- und -managementsysteme;
- Antriebs- und Maschinenmanagement und Leistungsregelungssysteme;
- Zugangskontrollsysteme;
- Passagierversorgungs- und -managementsysteme;
- für Passagiere zugängliche öffentliche Netzwerke;
- administrative und Versorgungssysteme der Besatzung; und
- Kommunikationssysteme.

2.1.2 Die Unterscheidung zwischen informationstechnologischen und betriebstechnischen Systemen sollte beachtet werden. Systeme der Informationstechnologie können betrachtet werden als Systeme, deren Fokus auf der Verwendung von Daten als Information liegt. Betriebstechnische Systeme können betrachtet werden als Systeme, deren Fokus auf der Verwendung von Daten für die Steuerung und Überwachung physikalischer Prozesse liegt. Darüber hinaus sollte auch der Schutz des Informations- und Datenaustauschs innerhalb dieser Systeme beachtet werden.

2.1.3 Obgleich diese Technologien und Systeme beträchtliche Effizienzzuwächse für die maritime Industrie bringen, stellen sie auch Risiken für kritische Systeme und Prozesse dar, die mit dem Betrieb der Schifffahrtssysteme verknüpft sind. Diese Risiken können aus Schwachstellen resultieren, die durch inadäquaten Betrieb, Integration, Instandhaltung und Konzeption cyberbezogener Systeme entstehen, sowie durch beabsichtigte und unbeabsichtigte Cyber-Bedrohungen.

2.1.4 Bedrohungen ergeben sich durch böswillige Handlungen (z. B. Hacking oder Eindringen von Malware) oder die unbeabsichtigten Folgen unkritischer Handlungen (z. B. Softwarewartung oder Nutzerberechtigungen). In der Regel legen diese Handlungen Schwachstellen auf (z. B. veraltete Software oder unwirksame Firewalls), oder sie nutzen eine Schwachstelle in der Betriebstechnik oder Informationstechnologie aus. Ein effektives Cyber-Risikomanagement sollte beide Arten von Bedrohung in Betracht ziehen.

2.1.5 Schwachstellen können aus Unzulänglichkeiten im Design, der Integration und/oder der Wartung der Systeme entstehen, sowie aus Nachlässigkeit in der Cyber-Disziplin. Generell gilt, in allen Fällen, in denen Schwachstellen in der Betriebstechnik und/oder Informationstechnologie entweder direkt (z. B. schwache Passwörter führen zu einem unberechtigten Zugriff) oder indirekt (z. B. fehlende Netzwerktrennung) aufgedeckt oder ausgenutzt werden, können Auswirkungen auf die Gefahrenabwehr und die Vertraulichkeit, die Integrität und Verfügbarkeit der Informationen entstehen. Wenn betriebstechnische und/oder informationstechnologi-

sche Schwachstellen aufgedeckt oder ausgenutzt werden, können darüber hinaus Auswirkungen auf die Sicherheit insbesondere in den Fällen eintreten, in denen kritische Systeme (z. B. die Brückennavigation oder die Hauptantriebssysteme) beeinträchtigt werden.

2.1.6 Ein effektives Cyber-Risikomanagement sollte auch Einflüsse auf die Sicherheit und Gefahrenabwehr berücksichtigen, die durch Aufdeckung oder Ausnutzung von Schwachstellen in informationstechnologischen Systemen entstehen. Diese könnten aus einem unsachgemäßen Anschluss an betriebstechnische Systeme oder Verfahrensfehlern von Bedienpersonal oder Drittparteien resultieren, die zur Gefährdung dieser Systeme führen kann (z. B. unsachgemäße Verwendung eines Wechseldatenträgers wie einen Memory-Stick).

2.1.7 Weitere Informationen bezüglich Schwachstellen und Bedrohungen sind den zusätzlichen Leitlinien und Standards zu entnehmen, die unter Abschnitt 4 aufgeführt werden.

2.1.8 Diese sich rapide verändernden Technologien und Bedrohungen machen es schwer, diese Risiken nur durch technische Standards zu behandeln. Daher empfehlen diese Richtlinien einen Ansatz für das Cyber-Risikomanagement, der widerstandsfähig ist und sich als natürliche Erweiterung der bestehenden Managementpraktiken zur Sicherheit und Gefahrenabwehr entwickelt.

2.1.9 Bei der Berücksichtigung potenzieller Quellen für Bedrohungen und Schwachstellen und damit verbundenen Risikominderungsstrategien sollten eine Reihe von potenziellen Kontrolloptionen für das Cyber-Risikomanagement in Betracht gezogen werden, die unter anderem das Management sowie betriebliche, Verfahrens- und technische Kontrollen umfassen.

2.2 Anwendung

2.2.1 Diese Richtlinien sind in erster Linie auf alle Organisationen in der Schifffahrtsindustrie ausgerichtet und sie verfolgen den Zweck, die Managementpraktiken zur Sicherheit und Gefahrenabwehr im Cyber-Bereich zu fördern.

2.2.2 In Anerkennung der Tatsache, dass nicht zwei Organisationen der Schifffahrtsbranche miteinander identisch sind, werden diese Anleitungen allgemeiner formuliert, um ihre umfassende Anwendbarkeit zu gewährleisten. Schiffe mit eingeschränkten cyberbezogenen Systemen werden eine einfache Anwendung dieser Richtlinien für ausreichend erachten; Schiffe mit komplexen cyberbezogenen Systemen können jedoch ein höheres Niveau an Sorgfalt verlangen und sollten deshalb zusätzliche Ressourcen durch etablierte Industrie- und staatliche Partner in Anspruch nehmen.

2.2.3 Diese Richtlinien haben Empfehlungscharakter.

3 Elemente des Cyber-Risikomanagements

3.1 Für den Zweck dieser Richtlinien meint das Cyber-Risikomanagement den Prozess der Identifikation, Analyse, Bewertung und Kommunikation eines cyberbezogenen Risikos und seiner Akzeptierung, Vermeidung, Übertragung oder Milderung auf ein annehmbares Niveau, wobei Kosten und Nutzen der Maßnahmen für die Beteiligten zu berücksichtigen sind.

3.2 Das Ziel des maritimen Cyber-Risikomanagements besteht darin, den Schutz und die Sicherheit in der Schifffahrt zu gewährleisten, die gegenüber Cyber-Risiken betrieblich widerstandsfähig ist.

3.3 Ein effektives Cyber-Risikomanagement sollte auf der Ebene des höheren Managements beginnen. Das höhere Management sollte eine Kultur des Cyber-Risikobewusstseins in allen Ebenen einer Organisation verankern und ein umfassendes und flexibles Regelwerk für das Cyber-Risikomanagement gewährleisten, das kontinuierlich im Einsatz ist und ständig durch effektive Rückkopplungsmechanismen bewertet wird.

3.4 Eine anerkannte Vorgehensweise, um obiges zu erreichen, besteht darin, die aktuellen und gewünschten Einstellungen des Cyber-Risikomanagements einer Organisation umfassend zu bewerten und zu vergleichen. Solch ein Vergleich kann Lücken aufdecken, die behandelt werden können, um die geforderten Risikomanagementziele durch einen nach Prioritäten gestaffelten Risikomanagementplan zu erreichen. Dieser risikobasierte Ansatz wird einer Organisation ermöglichen, seine Ressourcen auf die effektivste Weise einzusetzen.

3.5 Diese Richtlinien stellen die funktionalen Elemente dar, die das effektive Cyber-Risikomanagement unterstützen sollen. Diese funktionalen Elemente sind nicht sequenziell angelegt – alle sollten gleichzeitig und kontinuierlich in Gebrauch sein und sachgemäß in das Rahmenwerk des Risikomanagements eingeordnet werden:

.1 Identifizieren: Personalrollen und -verantwortlichkeiten für das Cyber-Risikomanagement definieren und die Systeme, Anlagen, Daten und Fähigkeiten identifizieren, die bei einer Unterbrechung für den Schiffsbetrieb ein Risiko darstellen.

.2 Schützen: Risikokontrollprozesse und -maßnahmen und eine Notfallplanung implementieren, um einem Cyber-Vorfall vorzubeugen und die Kontinuität des Schiffsbetriebs zu gewährleisten.

.3 Entdecken: Erforderliche Aktivitäten entwickeln und implementieren, um einen Cyber-Vorfall rechtzeitig zu entdecken.

.4 Reagieren: Aktivitäten und Pläne entwickeln und implementieren, um Widerstandsfähigkeit zu gewährleisten und die Systeme wiederherzustellen, die für die aufgrund eines Cyber-Vorfalls beeinträchtigten Schiffsbetriebs- oder Servicefunktionen notwendig sind.

.5 Wiederherstellen: Maßnahmen für die Unterstützung und die Wiederherstellung der Cyber-Systeme identifizieren, die für den von einem Cyber-Vorfall betroffenen Schiffsbetrieb erforderlich sind.

3.6 Diese funktionalen Elemente umfassen die Aktivitäten und die gewünschten Ergebnisse eines effektiven Cyber-Risikomanagements von kritischen Systemen, die die maritime Betriebsfähigkeit und den Informationsaustausch betreffen und einen fortlaufenden Prozess mit einem effektiven Rückkopplungsmechanismus darstellen.

3.7 Das effektive Cyber-Risikomanagement sollte auf allen Ebenen einer Organisation ein geeignetes Wachsamkeitsniveau gegenüber Cyber-Risiken gewährleisten. Das Wachsamkeits- und Bereitschaftsniveau sollte den Rollen und Verantwortlichkeiten im gesamten Cyber-Risikomanagementsystem entsprechen.

4 Bewährte Verfahren zur Implementierung des Cyber-Risikomanagements

4.1 Die hier beschriebene Vorgehensweise für das Cyber-Risikomanagement stellt eine Grundlage für das bessere Verständnis und den Umgang mit Cyber-Risiken dar, die damit einen Risikomanagementansatz ermöglicht, um mit Cyber-Bedrohungen und -Schwachstellen umzugehen. Für eine detaillierte Anleitung zum Cyber-Risikomanagement sollten die Nutzer dieser Richtlinien auch die jeweiligen Anforderungen der Mitgliedsstaaten und Flaggenstaatsverwaltungen zu Rate ziehen, sowie die einschlägigen internationalen und Industriestandards und bewährte Verfahren.

4.2 Zusätzliche Anleitungen und Standards können folgendes beinhalten, ohne darauf beschränkt zu sein:[1]

- Die „Guidelines on Cyber Security on board Ships“ von BIMCO, CLIA, ICS, INTERCARGO und INTERTANKO.
- ISO/IEC 27001 Standard über Informationstechnologie – Sicherheitstechniken – Informationssicherheitsmanagementsysteme – Anforderungen. Gemeinsam veröffentlicht von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC).
- United States National Institute of Standards and Technology‘s Framework for Improving Critical Infrastructure Security (the NIST Framework).

4.3 Verweise sollten stets auf die aktuellste Version der verwendeten Anleitung oder Standard erfolgen.

(VkBl. 2016 S. 738)

[1] Die zusätzlichen Anleitungen und Standards werden als eine nicht-vollständige Referenz auf weitere detaillierte Informationen für Nutzer dieser Richtlinien aufgelistet. Die aufgeführten Anleitungen und Standards wurden nicht von der Organisation herausgegeben, und ihre Verwendung liegt im Ermessen der jeweiligen Nutzer dieser Richtlinien.

Nachrichten für Seefahrer (NfS) – online

Information für die Berufsschifffahrt
Die vom Bundesamt für Seeschifffahrt und Hydrographie (BSH) herausgegebenen, digitalen NfS sind als amtliche Veröffentlichung anerkannt und werden deshalb nicht mehr kostenlos auf den Internetseiten des BSH (www.bsh.de) zur Verfügung gestellt.
Die digitalen NfS können online zum gleichen Preis wie das gedruckte NfS-Heft bezogen werden.

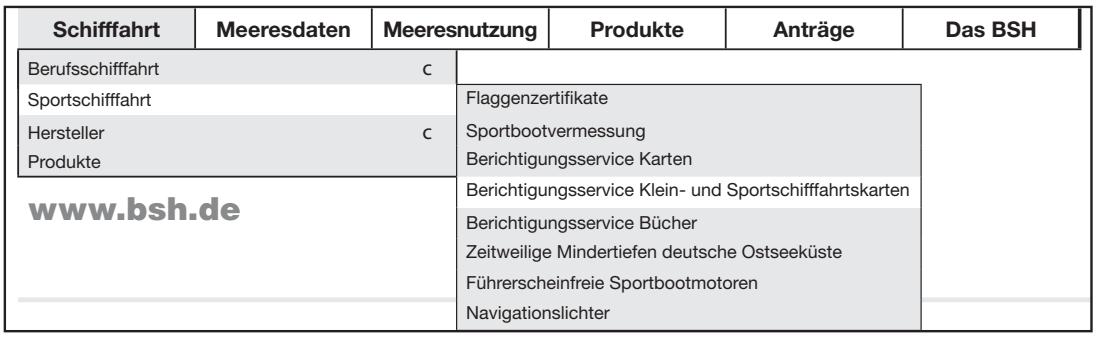
Information für die Klein- und Sportschifffahrt
Die Klein- und Sportschifffahrt kann den Berichtigungsservice (auch als Sammelberichtigungen bekannt) für die vom BSH herausgegebenen Seekarten, Sportbootkarten und nautischen Veröffentlichungen verwenden.

German Notices to Mariners (NfS) – online

Information to commercial shipping
The digitised Nachrichten für Seefahrer (NfS) on the BSH's website are official publications for which a fee is charged, as for the printed NfS.

Digitised Nachrichten für Seefahrer (NfS) are available at the same price as printed NfS.

Information to small craft and leisure shipping
Summaries of corrections to the navigational charts, small craft charts and publications issued by the BSH can be accessed on the BSH's website.



Die kostenlos zur Verfügung gestellten Sammelberichtigungen ersetzen nicht die amtlichen NfS.

Allgemeine Information
Die digitalen Nachrichten für Seefahrer werden online als eine gesamte NfS-Datei und in einzelnen Dateien angeboten (alle im PDF-Format):
– Teile 1–4 der NfS
– Beilagen zu den NfS
– Seekarten-Deckblätter in den NfS
Innerhalb der gesamten NfS-Datei und in der Datei Teile 1–4 sind im Navigationsfenster der Software von Adobe Acrobat Lesezeichen eingerichtet, die das gezielte Aufsuchen von Informationen erleichtern.
Der Schifffahrt wird empfohlen, die von der IMO angenommenen „Guidelines for the on-board use and application of computers – MSC/Circ.891" vom 21. Dezember 1998 zu beachten.

The summaries of corrections, which are available free of charge, do not replace the official NfS.

General information
The digitised Nachrichten für Seefahrer (NfS) in PDF format can be ordered completely or as:

– *parts 1 to 4*
– *enclosures*
– *chart blocks*

Within the files of the complete NfS and parts 1–4, the search for information is facilitated by icons on the Adobe Acrobat navigation window.

Mariners are advised to comply with the "Guidelines for the on-board use and application of computers – MSC/Circ.891" of 21 December 1998 which has been adopted by the IMO.