



Türk Loydu
Newsletter'in önceki
sayılarına
www.turkloydu.org
web sayfasından
ulaşabilirsiniz.

DENİZCİLİK SİBER RİSK YÖNETİMİ

2017 yılında, Uluslararası Denizcilik Örgütü (IMO), Emniyet Yönetimi Sistemlerinde (SMS) Denizcilik Siber Risk Yönetimi ile ilgili MSC.428 (98) kararını kabul etti. Kararda, onaylanmış bir SMS'nin, ISM Kodunun hedefleri ve işlevsel gereklilikleri uyarınca siber risk yönetimini dikkate alması gerektiği belirtildi. Ayrıca idareleri, siber risklerin şirketin 1 Ocak 2021'den sonra yapılacak "Uygunluk Dökümanı" (Document of Compliance)'nın ilk yıllık doğrulamasından önce SMS'de uygun şekilde ele alınmasını sağlamaya teşvik eder.

IMO ayrıca Denizcilik Siber Risk Yönetimine ilişkin rehber ise MSC-FAL.1/Circ.3 sirküleriyle yayınlanmıştır. Bu sirküler, halihazırda var olan risk yönetimi süreçlerine, siber risk yönetiminin dahil edilmesi için gereken tavsiyeleri içerir. Sirküler ayrıca etkili siber risk yönetimini destekleyen operasyonel unsurları da içerir.

Denizcilik siber riski; bir teknoloji varlığının, var olan bilgi veya sistemin bozulması, kaybolması veya tehlikeye atılması sonucunda, deniz taşımacılığı ile ilgili operasyonel, emniyet veya güvenlik arızalarına neden olabilecek potansiyel bir durum veya olay tarafından tehdit edildiği durumlarda alınacak önlemlere refere eder.

Kılavuz, etkili siber risk yönetimini destekleyen işlevsel unsurları aşağıdaki gibi sunar:

- Tanımlama: Siber risk yönetimi için personel rollerinin ve sorumlulukların belirlenmesi ve kesintiye uğradığında gemi operasyonları için risk oluşturan sistemler, varlıklar, veriler ve yeteneklerin tanımlanması.
- Koruma: Bir siber olaya karşı koruma sağlamak ve denizcilik operasyonlarının sürekliliğini sağlamak için risk kontrol süreçlerinin ve önlemlerinin ve acil durum planlamasının uygulanması.
- Tespit Etme: Bir siber olayı zamanında tespit etmek için gerekli faaliyetlerin geliştirilmesi ve uygulanması.
- Yanıtlama: Dayanıklılık sağlamak ve bir siber olay nedeniyle bozulan denizcilik operasyonları veya hizmetleri için gerekli sistemleri geri yüklemek için faaliyetler ve planlar geliştirilmesi ve uygulanması.
- Kurtarma: Bir siber olaydan etkilenen denizcilik operasyonları için gerekli siber sistemleri yedeklemek ve geri yüklemek için önlemlerin belirlenmesi.

Tavsiyeler

MSC.428 (98) kararları doğrultusunda, "Siber Güvenlik" ile ilgili politikalar, prosedürler, talimatlar, risk analizleri ve kontrol listeleri hazırlanmalı ve SMS'nin ilgili bölümlerine entegre edilmelidir. Hazırlanan döküman SMS'ye ek bir döküman da olabilir. Gemi işletmecileri ve/veya armatörler, 1 Ocak 2021'den sonra şirketin Uygunluk Dokümanı'nın ilk yıllık denetiminden önce belgeleri incelenmesi için zamanında Türk Loydu'nun Gemi Yönetim Sistemleri Birimi'ne teslim etmelidir.

Daha detaylı bilgi için:

Osman ÇAMÖZÜ
Gemi Yönetim Sistemleri Birimi Yöneticisi
Deniz Sektörü
Tel: +90 216 581 3868
Fax: +90 216 581 3810
E-mail: ocamozu@turkloydu.org
Web: www.turkloydu.org

LEGAL NOTICE All rights reserved.

The information contained here is for general information purposes only.

Türk Loydu shall be under no liability or responsibility in contract or negligence or otherwise howsoever to any person in respect of any information or advice expressly or impliedly given in this document, or in respect of any inaccuracy herein or omission here from or in respect of any act or omission which has caused or contributed to this document being issued with the information or advice it contains (if any).



Please log on
www.turkloydu.org
for previous issues of
Türk Loydu
Newsletter

MARITIME CYBER RISK MANAGEMENT

In 2017, the International Maritime Organization (IMO) adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management System (SMS). The Resolution stated that an approved SMS should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code. It further encourages administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

At the same time, IMO published "Guidelines on Maritime Cyber Risk Management" with circular MSC-FAL.1/Circ.3. This circular contains recommendations for incorporating cyber risk management into existing risk management processes. The circular also includes operational elements that support effective cyber risk management.

Maritime cyber risk refers to the measures to be taken in cases where a technology asset is threatened by a potential situation or event that may cause operational, safety or security failures related to maritime transport as a result of the breakdown, loss or compromise of existing information or systems.

The Guidelines present the functional elements that support effective cyber risk management as follows:

- Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.
- Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
- Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.
- Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.
- Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

Recommendation

In line with the decisions of MSC.428 (98), policies, procedures, instructions, risk analyzes and checklists related to "Cyber Security" should be prepared and integrated into the relevant parts of the SMS. The document prepared may also be an additional document to the SMS. Operators and shipowners should submit the documents in due course to Marine Management System Department of Türk Loydu for review of the documents before the first annual verification of the company's Document of Compliance after 1 January 2021.

For further information:

Osman ÇAMÖZÜ
Marine Management System Department Chief
Marine Sector
Tel: +90 216 581 3868
Fax: +90 216 581 3810
E-mail: ocamozu@turkloydu.org
Web: www.turkloydu.org

LEGAL NOTICE All rights reserved.

The information contained here is for general information purposes only. Türk Loydu shall be under no liability or responsibility in contract or negligence or otherwise howsoever to any person in respect of any information or advice expressly or impliedly given in this document, or in respect of any inaccuracy herein or omission here from or in respect of any act or omission which has caused or contributed to this document being issued with the information or advice it contains (if any).