İstanbul :
Sayı
Our Reference : 4687
Konu
Subject : Gemilerde Siber Güvenlik Rehberi'nin Yeni Versiyonu Yayımlandı

13.12.2018

Sirküler No: 737/2018

İlgi : Uluslararası Deniz Ticaret Odası (ICS)'nın 10.12.2018 tarihli ve MC(18)107 sayılı yazısı.

Uluslararası Deniz Ticaret Odası (ICS) tarafından gönderilen ilgi yazıda, Gemilerde Siber Güvenlik Rehberi üçüncü versiyonunun ICS web sayfasından; (http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16) ulaşılabileceği bildirilmektedir. Bir önceki sürüm üzerindeki değişikliklere ilgi yazı eklerinde (Annex A, Annex B) yer verildiği, Rehberin ekinde (Annex 2) siber güvenlik konularının mevzuata uygunluk açısından denizcilik firmalarına tavsiyeler içerdiğine dikkat çekildiği, ayrıca IMO gerekliliklerince şirketlerin 1 Ocak 2021 sonrası yıllık uygunluk belgesi doğrulamasında siber risk yönetimlerini, güvenli yönetim sistemleriyle birleştirebilmelerine yardımcı olmak üzere dizayn edildiği belirtilmektedir.

Rehber ile ilgili görüş ve sorularınız varsa ICS'e iletilmek üzere Odamıza (serkan.inal@denizticaretodasi.org.tr) gönderilmesi hususunda bilgilerinizi arz ve rica ederiz.

Saygılarımızla,

Murat TUNCER
Genel Sekreter

EKLER:
EK-1: Kılavuzdaki Yenilikler Türkçe Çevirisi (1 sayfa)
EK-2: İlgi yazı ve Eki (1 sayfa)

DAĞITIM:

Gereği:
-Tüm Üyelerimiz (Web Sayfasında)
-Türk Armatörler Birliği
-S.S. Gemi Armatörleri Mot. Taş. Koop.
-Vapur Donatanları ve Acenteleri Derneği
-GİSBİR
-GESAD
-Gemi ve Yat İhracatçıları Birliği
-Türk Loydu Uygunluk Değerlendirme Hizmetleri A.Ş.
-KOSTBİR
-UND
-İMEAK DTO Şubeleri ve Temsilcilikleri
-Gemi Yakıt İkmalciler Derneği
-S.S. Deniz Tankerleri Akaryakıt Taş. Koop.
-Gemi Brokerleri Derneği

Bilgi:
-Meclis Başkanlık Divanı
-Yönetim Kurulu Başkan ve Üyeleri
-WISTA Türkiye Derneği

Ayrıntılı Bilgi: Serkan İNAL **Telefon:** +90 212 252 01 30/157 **e-mail:** serkan.inal@denizticaretodasi.org.tr

-Gemi Tedarikçileri Derneği
-KOSDER
-ROFED
-KOGAD
-İ.T.Ü. Denizcilik Fakültesi Mezunları Derneği
-Türk Uzakyol Gemi Kaptanları Derneği
-Türk Kılavuz Kaptanları Derneği
-Gemi Makineleri İşletme Mühendisleri Odası
-Gemi Mühendisleri Odası
-Özel Denizcilik Kursları Derneği
-Gemi Sahibi Firmalar
-Tüm Acenteler

EK-1

Serbest Çeviri
(13.12.2018)

(BIMCO tarafından hazırlanmıştır.)

Gemilerde Siber Güvenlik Kılavuzu 3. Versiyonu'ndaki Yenilikler

Güvenlik Yönetimi Sistemi (SMS) Deniz Siber Risk Yönetimi ile ilgili MSC.428 (98) sayılı IMO kararı, onaylanmış bir SMS'nin, ISM Kodunun hedefleri ve işlevsel gerekliliklerine uygun olarak siber risk yönetimini dikkate alması gerektiğine işaret etmektedir. Siber risk, bir geminin güvenli çalışmasını ve çevrenin korunmasını etkileyebilecek diğer risklerle aynı şekilde değerlendirilmelidir. Siber risk yönetiminin şirketin SMS'sine nasıl dahil edileceğine dair göz önünde bulundurulması gereken özel ve işlevsel konular ile önlemler kılavuza dahil edilmiştir.

Bir geminin küresel tedarik zincirinin ayrılmaz bir parçası olduğu göz önüne alındığında, kılavuzun 3.sürümü; gemi sahibi, gemi acentesi, gemi işletmesi, satıcılar ve tedarik zincirindeki diğer taraflar arasındaki ilişkide siber risklerin nasıl yönetileceğine dair rehberlik içerir. Bu ilişkiler sadece güvene dayalı değil, aynı zamanda karşılıklı olarak kabul edilebilir bir siber risk yönetimi düzeyine dair, ortak bir anlayışa da dayanmalıdır.

Operasyonel teknik sistemler (OT) ve bilgi teknik sistemleri (IT) arasındaki farklar belirlenmiştir. OT, fiziksel aygıtları ve süreçleri doğrudan izleyen / kontrol eden donanım ve yazılımlardır. Bilgi işlem ise donanım ve iletişim teknolojileri dahil olmak üzere teknolojiler yelpazesini kapsamaktadır. Kılavuz, gemi sahiplerinin, bir şirkette yönetim ve satın alma stratejilerinin kapsamlı bir şekilde ele alınmasını sağlamaya yardımcı olmak üzere IT ve OT arasındaki engellerin kaldırılması gerekliliğine dikkat çekmektedir. Güvenlik değerlendirmesine gelince, fiziksel dünyanın ve dijital dünyanın artık iç içe geçtiği akılda tutulmalıdır.

NotPetya saldırısından öğrenilen derslerden biri de, geminin OT'sinin, gerektiğinde siber saldırı sırasında kıyı bağlantılarına derhal sonlandırabilmesine olanak sağlayacak rehberliğe ihtiyaç olduğunu göstermiştir. Geminin güvenli bir şekilde işlerliğini sağlamak adına bazı sistemlerin sürekli kullanımına ihtiyaç duyulmaya bilir, ancak bu sistemler geminin güvenliğini tehdit edebilecek siber saldırılara olanak sağlamak üzere kullanılabilir.

Rehberde, siber güvenlik saldırılarına nasıl yanıt verileceği ve olası saldırı sonrası sistemin nasıl geri kazanılabileceği ile ilgili bölümü yenilendi.

Siber Güvenlik ile ilgili potansiyel sorunlara vurgulamak için, kılavuzun ilgili bölümlerine, gemilerde yaşanan yedi siber güvenlik olayı eklenmiştir. Söz konusu olaylar göstermektedir ki denizciler arasında farkındalığın oluşturulması ile bazı siber güvenlik tehditleri kolaylıkla bertaraf edilebilmektedir.

Sonuç olarak, Rehberin 3. Versiyonunda son gelişmelere bağlı olarak pratik düzenlemeler geliştirilmiştir.

EK-2

International Chamber of Shipping
Shaping the Future of Shipping

38 St Mary Axe London EC3A 8BH

Tel +44 20 7090 1460
Fax +44 20 7090 1484

info@ics-shipping.org | ics-shipping.org

10 December 2018 **MC(18)107**

TO: MARINE COMMITTEE

Copy: All Full and Associate Members (for information)

PUBLICATION OF VERSION 3 OF THE INDUSTRY GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

Action required: ***Members are advised of the publication of version 3 of the industry Guidelines on Cyber Security Onboard Ships, and are invited to disseminate this information as widely as possible amongst Companies and Administrations.***

Members are advised that version 3 of the industry *Guidelines on Cyber Security Onboard Ships* (the Guidelines) is now available on the ICS website.

Version 3 of the Guidelines and a summary of the changes are attached at **Annex A** and **Annex B**, respectively. A more detailed summary of updates was provided in MC(18)94.

From the perspective of regulatory compliance, Members attention is drawn to the advice in annex 2 of the Guidelines. This is designed to help Companies incorporate cyber risk management (based on the IMO *Guidelines on Maritime Cyber Risk Management* (MSC-FAL.1/Circ.3)) into safety management systems by the first annual verification of the company's Document of Compliance after 1 January 2021. This is required by IMO resolution MSC.428(98).

Members are requested to draw the attention of their Administrations to this Guidance with a view to aligning Administrations' expectations and requirements with the industry's guidance on cyber risk management. The verbal report of the publication of version 3 of the Guidelines was made by BIMCO to MSC 100 last week.

Any questions or comments on version 3 of the Guidelines should be sent to the undersigned (matthew.williams@ics-shipping.org).

Matthew Williams
Senior Marine Adviser

(Prepared by BIMCO)

New items in version 3 of The Guidelines on Cyber Security Onboard Ships

The IMO resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management System (SMS) stated that an approved SMS should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code. Cyber risk should be addressed in the same way as any other risk that may affect the safe operation of a ship and protection of the environment. Specific and actionable guidance and measures to consider on how to incorporate cyber risk management into the company's SMS have been incorporated into the guidelines.

Considering that a ship is an integral part of the global supply chain, version 3 includes guidance on the how to manage cyber risks in the relationship between the shipowner, ship agent, ship manager, vendors and other parties in the supply chain. These relationships should not only be based on trust but also a common understanding of a mutually acceptable level of cyber risk management.

The difference between operational technical systems (OT) and information technical systems (IT) has been elaborated. OT is hardware and software that directly monitors/controls physical devices and processes, whilst IT covers the spectrum of technologies for information processing and data handling including software, hardware and communication technologies. The guidelines encourage that shipowners give consideration to remove barriers between IT and OT to help ensure management and procurement strategies are handled comprehensively in a company. When it comes to the safety assessment, the possible effect that OT has on the the physical world should be taken into account bearing in mind that the physical and the digital worlds are now intertwined.

Lessons learnt from the NotPetya attack showed the need for guidance on the immediate disconnection of the ship's OT to shore connections during a cyber attack, as appropriate and where required. Some systems may not be strictly necessary for operating the ship safely, but they could represent a potential attack vector to the systems that are required for the ship's safe operation. Furthermore, the chapter on how to respond to and recover from cyber security incidents has been updated.

Seven verified cyber incidents onboard ships have been added to the appropriate sections of the guidelines to highlight and illustrate potential problems. The impact of these incidents demonstrates the need to raise awareness among seafarers as some could have been easily avoided.

In conclusion, the level of practical guidance in version 3 has been increased in accordance with recent developments.