İSTANBUL VE MARMARA, EGE, AKDENİZ, KARADENİZ BÖLGELERİ
DENİZ TİCARET ODASI
İSTANBUL & MARMARA, AEGEAN, MEDITERRANEAN, BLACKSEA REGIONS
CHAMBER OF SHIPPING

İstanbul :
Our Reference : 3120

14.08.2017

Konu
Subject : **Siber Güvenlik 2021'den itibaren Uluslararası Güvenli Yönetim (ISM) kodunun bir kısmı Olacaktır.**

Sirküler No: 536 / 2017

Sayın Üyemiz,

İlgi: 07.07.2017 tarihli TradeWinds gazetesinde yayınlanan bir yazı.

İlgi yazıda, tüm güvenlik risklerinin belirlenmesini ve buna göre davranılmasını gerektiren kuralların halen mevcut olmasına rağmen, Siber Güvenliğin 2021'den itibaren Uluslararası Güvenli Yönetim (ISM – International Safety Management) kodunun resmen bir kısmı olacağı belirtilmektedir.

Haziran 2017'de yapılan IMO Deniz Emniyeti Komitesi (IMO MSC) toplantısında birçok delege, gemiler için olan tüm risklerin belirtilmesini şart koşan ISM Kodunun mevcut zorunlu gereksinmelerine siber tehlikelerin halen dahil edilmiş olduğunu öne sürmüştür. Bununla birlikte, kısa zaman içinde yayınlanacak olan IMO Kurallarının zorunlu değil fakat tavsiye şeklinde olacağı, 2021 uygulama son tarihine rağmen, İdarelerin riski tam olarak nasıl yöneteceklerini kararlaştırmalarının gerekeceği belirtilmektedir.

İlgi yazının Odamızda yapılan Türkçe çevirisi (Ek-1) ve İlgi yazı (Ek-2) ilişikte sunulmuştur.

Bilgilerinizi arz ve rica ederiz.

Saygılarımızla,

Murat TUNCER
Genel Sekreter

EKLER:

Ek-1: İlgi yazının Türkçe çevirisi

Ek-2: İlgi Yazı

Ayrıntılı Bilgi : Engin KÖKNEL
E-mail engin.koknel@denizticaretodasi.org.tr
Telefon : +90 212 252 01 30 / 246

İstanbul : 14.08.2017
Our Reference :

Konu
Subject : **Siber Güvenlik 2021'den itibaren Uluslararası Güvenli Yönetim (ISM) kodunun bir kısmı Olacaktır.**

DAĞITIM:

Gereği:

-Tüm Üyelerimiz (Web)
-Türk Armatörler Birliği
- S/S Gemi Armatörleri Motorlu Taş. Koop.
-Vapur Donatanları ve Acenteleri Derneği
-İMEAK DTO Şubeleri
-GİSBİR
-TÜRKLİM
-UTİKAD
-GESAD
-Gemi Brokerleri Derneği
-Türk Loydu
-Türk Uzakyol Gemi Kaptanları Derneği
-Gemi, Makineleri İşletme Mühendisleri Odası
-Gemi Mühendisleri Odası
-Gemi Sahibi Firmalar

Bilgi:

-Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
Deniz ve İçsular Düzenleme Genel Müdürlüğü
-Sn. Sefer KALKAVAN
TOBB DTO'ları Konsey Başkanı
-Meclis Başkanlık Divanı
-Yönetim Kurulu Başkanı ve Üyeleri
-Sn. Erol YÜCEL
TOBB Türkiye Denizcilik Meclisi Başkanı
-Piri Reis Üniversitesi
-TAİS
-WISTA Türkiye Derneği

Ayrıntılı Bilgi : Engin KÖKNEL Telefon : +90 212 252 01 30 / 246
E-mail engin.koknel@denizticaretodasi.org.tr

EK-1

(Serbest çeviridir)

SİBER GÜVENLİK - IMO BAYRAK VE LİMAN DEVLETLERİNİN GERÇEKLEŞTİRMESİ İÇİN 2021 SON TARİHİNİ SAPTIYOR

Paul Berrill Londra'dan bildiriyor.

Tüm güvenlik risklerinin belirlenmesini ve buna göre davranılmasını gerektiren kuralların halen mevcut olmasına rağmen, siber güvenlik 2021'den itibaren Uluslararası Güvenli Yönetim (ISM – International Safety Management) kodunun resmen bir kısmı olacaktır.

Uluslararası Denizcilik Örgütü (IMO) Deniz Emniyeti Komitesi (MSC) geçenlerde, " 1 Ocak 2021 sonrası şirketin uygunluk dokümanının birinci yıllık onaylanmasından daha geç olmamak üzere " bayrak ve liman devletlerini siber güvenlik risklerini belirtmeye teşvik etmeyi kararlaştırmıştır.

Bu karar NotPetya kötü amaçlı yazılım (malware) saldırısından sadece birkaç gün önce kabul edilmiştir. Bu saldırı, dünyadaki birçok belli başlı AP Moller-Maersk liman terminallerindeki operasyonları kesintiye uğratmış, milyonlarca dolarlık potansiyel kayıplara sebep olmuştur.

Haziran ayında yapılan IMO Deniz Emniyeti Komitesi (IMO MSC) toplantısında birçok delegeler, gemiler için olan tüm tanımlanan risklerin belirtilmesini şart koşan ISM Kodunun mevcut zorunlu gereksinmelerine siber tehlikelerin halen dahil edilmiş olduğunu öne sürmüşlerdir.

Ancak, kısa zaman içinde yayınlanacak olan IMO Kuralları zorunlu değil fakat tavsiye şeklinde olacaktır. 2021 uygulama son tarihine rağmen, İdarelerin riski tam olarak nasıl yöneteceklerini kararlaştırması gerekecektir.

SİSTEMLER ÜZERİNE ODAKLANMA

İlaveten, tavsiyeler büyük ölçüde gemi sistemleri üzerine odaklanmaktadır, bu da eleştirmenlerin APM Terminalleri vakasında olduğu gibi, bunların sektörün bütünleştirilmiş bilgisayar şebekeleri üzerine olan bir saldırının etkisini belirtmeyi başaramadıklarını öne sürmektedirler.

Bununla birlikte, yol gösterici kurallar, - Maersk'in başlangıçta mücadele ettiği - iş (business) sistemlerini ve denizcilik operasyonlarını iyileştirmek için olan planları kapsayacak şekilde yukarıdan aşağıya (top-down) bir yaklaşımla siber güvenliğin yönetim ileri gelenleri tarafından ele alınmasına olan ihtiyacı vurgulamaktadır.

IMO kuralları, ABD'deki Teknoloji Standartları Ulusal Enstitüsü gibi, hükümet örgütleri tarafından çıkarılan bilgileri büyük ölçüde yansıtmaktadır.

İdareler önce NotPetya'nın fidye işi olduğunu farz etmişlerdir, ancak daha sonra bunun kötü niyetle yapılan, muhtemelen siyasi yönü olan, Ukrayna'ya karşı yapılmış bir darbe olduğu belirlenmiştir, bu zorla para koparmaya karşı kurbanın veri dosyalarını silmek için düzenlenmişti.

Uzmanlar, NotPetya'nın yaratıcılarının, İdareleri bununla mücadele teşebbüslerinde yanıltmak için, kodu Petya fidye yazılımlarından (ransomware) ödünç aldıklarına inanmaktadırlar. Fidye yazılımı (Ransomware), veriyi zedelemek üzere bir ödeme yapılmasını otomatik hale getirmek için, genellikle her bir enfeksiyon kapmış bilgisayarı eşsiz gizli nakit para (cryptocurrency) çanta bölümlerine (wallets) bağlamaktadır; ancak, NotPetya tek bir çanta bölümüne (wallet) bağlı idi – bu da ödemeyi konu dışı bırakmıştır.

(07.07.2017 tarihli TradeWinds gazetesinde yayınlanmıştır.)

Çeviren: Engin KÖKNEL
Dış İlişkiler Bölüm Müdürü

vice-president of maritime security consultant Hudson Trident in a Viewpoint article

EK-2

Last week's NotPetya cyber attack against Maersk's ship and port enterprise is more than a "wake-up call", it is a fresh example of the existential risk that cyber threats pose to shipping companies.

Shipping groups can no longer afford to wait passively for requirements levied by national authorities or the International Maritime Organization (IMO) but must initiate cyber-security measures out of self-preservation.

This approach will benefit in several ways, including the potential to shape additional guidance and the ability to embed cyber into broader enterprise security and resilience. A mature cyber-security approach could provide a competitive advantage.

The IMO released a circular detailing how cyber security should be addressed in general terms for ships but not ports just days before the NotPetya attack. The IMO guidance indicates that cyber security and risk management will be required to be taken into account in implementation of the International Ship Management code by 2021.

National governments are also in the process of determining to what level they should regulate cyber security as port and flag states, and the US Coast Guard is in the final stages of reviewing guidance. It has already released a policy letter into how transportation security incidents and breaches of security that involve a cyber component should be reported.

Senior executives of shipping companies or ports are likely to have placed responsibility for cyber security on their information technology departments or outsourced this responsibility. This may be because cyber security has an element of mystique that can complicate their ability to develop a clear understanding of the importance of the systems and risks to the enterprise that poor cyber security may bring.

For ships and ports, the risks are numerous. They generally involve unauthorised access to, or manipulation of, data or information that can be used to facilitate illegal activity including trafficking of contraband, cargo theft and sabotage.

These in turn bring broader risks around the ability to satisfy customers' delivery requirements, compliance with customs laws and supply-chain security programmes, reputational risk, and ultimately the potential loss of business and corporate value.

For complex organisations, it is imperative that someone in the C-Suite has an understanding of cyber risks and has a clear responsibility to oversee security. This requires companies to adopt a 'converged' security approach where physical, operational, and digital security are treated as interdependent.

This approach is likely to be challenging for many groups as chief security officers are often retired police or military personnel with a good knowledge of operational and physical security but a limited understanding of cyber risks. Conversely, IT managers are likely to have a good understanding of the technical issues but not necessarily of operational and physical security.

There are several steps that top maritime management can take:

BEGIN NOW: Waiting for the IMO or governments to provide guidance will exacerbate a company's exposure to attacks. There are internationally recognised standards that can be adapted for ships and ports. It is likely that any future guidance will reflect those key standards.

ENTERPRISE APPROACH: Cyber risks can affect all elements of a company including human resources, terminal and cargo operating systems, access control, communications, cargo tracking, financial databases and supervisory control and data acquisition.

TAKE TIME: A maturity model is recommended allowing companies to incrementally increase cyber security in a deliberate, enterprise-wide manner. This also allows better planning of budgetary requirements.

Cyber security and resilience are key components of enterprise today and should not be relegated to lower levels without top management engagement and oversight.

IMO sets 2021 deadline for flag and port states to act

Paul Berrill
London

Cyber security will formally become a part of the International Safety Management (ISM) code from 2021, despite the rules already requiring all security risks to be identified and acted on.

The international Maritime Organization (IMO) Maritime Safety Committee (MSC) recently agreed to encourage flag and port states to address cyber security risks "no later than the first annual verification of the company's document of compliance after 1 January 2021".

The resolution was agreed just days before the NotPetya malware attack that disrupted operations at several major AP Moller-Maersk port terminals around the world — causing potential losses of many millions of dollars.

Many delegates at the MSC session held in June argued that cyber threats are already included in the current mandatory requirements of the ISM code that stipulate all identified risks to shipping be addressed.

However, the soon to be published IMO guidelines will not be mandatory but recommended. Despite the 2021 implementation deadline, administrations will be left to decide exactly how they manage the risk.

FOCUS ON SYSTEMS

In addition, the recommendations largely focus on vessel systems, which led critics to claim that they fail to address the impact of an attack on the sector's integrated computer networks, as was the case with APM Terminals.

The guidelines do, however, stress the need for cyber security to be addressed by senior management with a top-down approach that encompasses business systems and recovery plans to restore shipping operations — which Maersk struggled with initially.

The IMO guidelines largely mirror the advice generated by government organisations such as the National Institute of Technology Standards in the US.

The authorities first assumed that the NotPetya was ransomware, but it was later identified as a malicious, possibly politically-motivated, strike against Ukraine, which was designed to wipe victim's data files as opposed to extorting money.

Experts believe that the creators of NotPetya borrowed code from Petya ransomware in a bid to confuse the authorities in their attempts to combat it. Ransomware usually links each infected computer to unique cryptocurrency wallets to automate a payment for data decryption, but NotPetya was linked to a single wallet — making payment irrelevant.

TradeWinds, 7.07.2017