Siber Riskler

Bugüne kadar daha çok filmlerde/ haberlerde gördüğümüz ve duyduğumuz Siber Saldırılar yavaş yavaş hayatımızın bir parçası olmaya başladı ve şirketler açısından da risk planlamalarında ön sıralara yerleşti. Denizcilikte tetikleyici faktör Haziran 2017'de siber saldırı altında kalan Maersk'in kaybını US$300 milyon olarak açıklaması sonrası gerçekleşti ve konu üzerinde denizciliğe özel seminerler ve çalıştaylar arttı.

Bu konuda IMO siber risk yönetimi tavsiyeleri baz alınarak neredeyse tüm büyük organizasyonlar (BIMCO, Intertanko, Interkargo, Iumi, vb) üyelerine benzer tavsiyeler yayınladılar. Sigorta açısından da sigorta teminatına girmeyen siber risklerle ilgili yine bazı sigortacıların, üye armatörlerine siber güvenlikte uzman şirketleri tavsiye ettiği, yeni ürünler sunduğu görülmektedir.

Peki ama gerçekten ne kadar risk altındayız? Bu sorunun cevabı hem çok hem az olarak değerlendirilebilir. Bugüne kadar filmlerde görüldüğü şekliyle doğrudan herhangi bir şirkete veya gemilere yönelik bir saldırı görülmemiştir. Diğer bir deyişle gemi sistemlerinin etkisiz hale getirilmesi veya geminin kontrolünün ele geçirilmesi şeklinde bir saldırı ile karşılaşılmamıştır. Stuxnet virüsü gibi belirli bir amaç için geliştirilmiş ve ülkelerin alt yapılarını hedef alan saldırılar zaten konumuzun dışında olup, şirketlerin bu şekilde sofistike saldırılara tek başlarına karşı koymaları da mümkün gözükmemektedir. Ancak günümüzde şahıs ve şirketlerin karşılaştığı temel siber riskler Petya, NotPetya, WannaCry, Equifax, vb. gibi virüsler yoluyla daha çok bilgi hırsızlığı veya datayı bloke ederek para talep edilmesi şeklindedir. Örneğin WannaCry virüsü, bilgisayarın hard diskini şifreleyerek erişime engellemesi ve deşifre ederek tekrar kullanıma açmak için belirli tutarda para istenmesi şeklinde çalışmaktadır. Petya ve sonrasında NotPetya virüsleri de benzer şekilde bilgisayardaki datalara ulaşımı engelleyerek, engeli kaldırmak için ücret talep edilmesi yöntemini izlemektedir.

Halil Solak
Teknik Müdür Yardımcısı
+90 216 545 0300 (D.236)
+90 533 200 2818
halil.solak@turkpandi.com

1977 yılı İstanbul doğumludur. Darüşşafaka Lisesi'nden 1995 yılında, İTÜ Denizcilik Fakültesi Güverte Bölümünden 1999 yılında mezun oldu. Zodiac Shipping'de deniz hayatına başladı. İTÜ Deniz Ulaştırma İşletme Mühendisliğinde yüksek lisans dersleri aldı. ABD Georgia State University'de Risk Yönetimi ve Sigorta alanında MBA yaptı. ABD Hartsfield Atlanta hava alanında ve Türkiye'de bazı önemli sigorta şirketlerinin Nakliyat Departmanlarında çalıştı. OMNI Brokerlik'te 9 yılın ardından 2015 yılında Türk P ve I Sigorta A.Ş. ailesine Teknik Müdür Yardımcısı olarak katıldı. Lojistikte Risk Yönetimi üzerine seminerler verdi.

TÜRKP&I

Burada ilginç olan, NotPetya'nın Ukrayna merkezli bir muhasebe yazılımı ile yayılmasıdır. Maersk'i etkileyen ve işletim zararları ile birlikte $300 milyonu bulan zararın sebebi NotPetya'dır. Yine Equifax ise Amerika Birleşik Devletlerinde kredi verilerini depolayan büyük bir kuruluştur. Siber saldırı ile Equifax'da kayıtlı kullanıcı verileri halka açılmıştır.

Bireysel kullanıcı veya küçük ve orta ölçekli bir şirket olarak , kullandığınız muhasebe yazılımından kaynaklı bir virüsü nasıl engelleyebilirsiniz, piyasadan satın aldığınız 100 TL'lik genel anti virüs programları ne kadar sizleri bu tür saldırılara karşı korur değerlendirmek gerekir. Günümüzde Siber Risk Sigortaları bulunmakla birlikte, normal risklerden ayrı bir risk analizi içerdiğinden Türkiye'de henüz yaygın olarak temin edilememektedir.

Yukarıda anlatılanlardan da anlaşılacağı üzere bu saldırılar genel, tüm bilgisayar kullanıcılarına yönelik olup denizcilik sektörü özelinde bugüne kadar yapılan bir siber saldırı yoktur. Ancak her Tekne& Makine poliçesinde, ana teminatlar kadar önem verilmeyip dikkatlerden kaçsa da , bir Siber Risk klozu yer almaktadır. 'Institute Cyber Attack Exclusion Clause Cl.380). Bu klozun tam metni internette kolayca bulunabilir, ancak özetlemek gerekirse Siber Riskler teminat harici bırakılmaktadır.

P&I sigortalarında ise durum biraz daha farklıdır. P&I sigortaları Belgesiz Ticaret (paperless trading) ile ilgili detaylı maddeler içerse de Siber Riskler ile ilgili henüz bir çalışma yapılmamıştır. Diğer bir deyişle gemiye yapılan bir siber saldırı durumunda bir sorumluluk oluşursa P&I teminatı, diğer herhangi bir sorumluluk hasarı gibi devreye girecektir. Bunun tek istisnası konu saldırının Harp ve Terör Riskleri kapsamına girmesidir.

Konuyu biraz daha açacak olursak; yakın zamana kadar gemiler açık denizde seyir halinde iken kara ile çok kısıtlı bağlantıları vardı, günümüzde ise AIS, ECDIS, GPS vb. birçok araç ile kara tesisleri ile elektronik bağlantıyı devam ettirmekte ve bu şekilde de siber risklere geçmişe kıyasla daha açık hale gelmektedirler. Bugüne kadar gerçekleşmemiş olsa da bir siber saldırı neticesinde gemi elektronik cihazları devre dışı kalıp, bunun sonucunda bir çatma, çevre kirliliği, üçüncü kişilere veya mallarına zarar verilmesi gibi P&I kapsamına giren bir hasar ortaya çıkarsa P&I sigortacıları devreye girerek oluşan zararı tazmin edeceklerdir. Ancak konu saldırı neticesinde geminin kendisine gelecek zararlar teminat dışıdır.

Basit gözükse de siber saldırılara karşı uzmanların öncelikli önerisi, gelen emaillerdeki ekleri açmadan önce iki kez düşünmek ve para transferi yapmadan önce sizlere gelen banka detaylarını telefonla da teyid etmek olarak ortaya çıkmaktadır.