T.C.
DOKUZ EYLÜL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
DENİZ ULAŞTIRMA İŞLETME MÜHENDİSLİĞİ
ANABİLİM DALI
DENİZCİLİKTE EMNİYET, GÜVENLİK VE ÇEVRE YÖNETİMİ
YÜKSEK LİSANS PROGRAMI
YÜKSEK LİSANS TEZİ

DENİZCİLİKTE SİBER GÜVENLİK: TÜRK GEMİ İŞLETMECİLERİ ÜZERİNE BİR İNCELEME

Onur TOPAL

Danışman
Dr. Ögr. Üyesi Burak KÖSEOĞLU

İZMİR - 2020

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum “Denizcilikte Siber Güvenlik; Türk Gemi İşletmecileri Üzerine Bir İnceleme” adlı çalışmanın, tarafımdan, akademik kurallara ve etik değerlere uygun olarak yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

Tarih

-/-/2020

Onur TOPAL

İmza

ÖZET

Yüksek Lisans Tezi
Denizcilikte Siber Güvenlik; Türk Gemi İşletmecileri Üzerine Bir İnceleme
Onur TOPAL

Dokuz Eylül Üniversitesi
Sosyal Bilimler Enstitüsü
Deniz Ulaştırma İşletme Mühendisliği Anabilim Dalı
Denizcilikte Emniyet, Güvenlik ve Çevre Yönetimi Yüksek Lisans Programı

Denizcilikte, güvenlik en önemli unsurların başında gelmektedir. Denizcilik sektörünün her alanında teknolojinin payı oldukça yüksektir, bu durum paralel olarak yapılacak olan siber saldırılara karşı güvenlik önlemlerinin önemini göstermektedir. Güvenlik önlemleri alınmamış sistemlerde doğabilecek sonuçlar oldukça ağır maddi ve manevi hasarlara sebebiyet verir. Dolayısıyla siber saldırıları tanımak, olabilecek saldırılara karşı önlemlerin önceden alınması oldukça önem arz etmekte olup bu konuda en zayıf nokta ise insan faktörüdür. Eğitimli ve farkındalığı yüksek personel istihdamı alınabilecek en önemli önlemdir. Denizcilik sektörünün bu konuda yapacağı yatırımlar ile personel farkındalığının artırılması gerekmektedir.

Bu çalışmada siber saldırı çeşitleri, gemi, şirket ve limanların bilgi alışveriş yöntemleri, gemilerde kullanılan siber saldırılara uğrayabilecek cihazların özellikleri incelenmiştir. Türk gemi işletmecilerindeki ilgili departman yetkilileriyle görüşmeler yapılmış ve durum analizleri tamamlanmıştır. Yapılan analizler sonucunda şirketlerin ve dolayısıyla gemilerin siber güvenlik hususunda yeterince önlem almadığı gözlemlenmiş ve bu duruma yeterince kaynak ayrılmadığı tespit edilmiştir. Kaynak ayrılmaması, personel eğitiminde ve yazılım yetersizliğine sebebiyet vermekte olup siber güvenlik konusunda ciddi zafiyetlere yol açmaktadır.

Anahtar Kelimeler: Denizcilik, Güvenlik, Siber Saldırı, İletişim, Yazılım

ABSTRACT

Master's Thesis

Maritime Cybersecurtiy: An Analyses On Turkish Shipping Companies

Onur TOPAL

Dokuz Eylul University

Graduate School of Social Sciences

Department of Marine Transportation Engineering

Maritime Safety, Security and Environmental Management Program

Security is major important thing in maritime industry. Technology has big share at maritime and it is explain to us how is important technological security importance. If there are no any precautions for cyber attack, it will cause to serious financial and moral damage. To understand cybersecurity and make necessary precautions becomes more important. At this point researches said that, Human is weakest link at this network. Educated and awareness crew is the best precautions for prevent this attacks. Maritime sector should make investment to cyber security for impove awerness.

At this study, cyber attack types, ship/port/companies network types, ship equipments specifications researched with details on security manners. Interview has been helded and analyzed with Turkish shipping companies. Analyses shows that, companies not get preventive measures for cyber security enougly and there are not enough fund for its. Inadequte fund causes less crew training and unqualified software. It's lead to low cyber security level.

Keywords: Maritime, Security, Cyber Attacks, Network, Software

DENİZCİLİKTE SİBERGÜVENLİK; TÜRK GEMİ İŞLETMECİLERİ ÜZERİNE BİR İNCELEME

İÇİNDEKİLER

İKİNCİ BÖLÜM

SİBER SALDIRIYA UĞRAYABİLECEK KÖPRÜSTÜ CİHAZLARININ YAPISI

ÜÇÜNCÜ BÖLÜM

GEMİ SİBER ATAK SENARYOLARI

DÖRDÜNCÜ BÖLÜM

TÜRK GEMİ İŞLETMECİLERİ ÜZERİNE İNCELEME

KISALTMALAR

AIS	Automatic Information System
AVCS	Admiralty Vector Chart Service
C & C	Command and Control
DOS	Denial of Service
ECDIS	Elektronic Chart and Display Informtion System
ENC	Electronic Nautical Chart
GPS	Geographical Positioning System
HTTP	Hypertext Transfer Protocol
IMO	International Maritime Organisation
IP	Internet Protocol
ITU	International Telecomunication Union
KVKK	Kişisel Verilerin Korunması Kanunu
LAN	Local Area Network
NMEA	National Marine Electronics Association
P&I	Protection and Indemnity
UDHB	Ulaştırma Denizcilik Ve Haberleşme Bakanlığı
VDR	Voice And Data Recorder

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

EKLER LİSTESİ

GİRİŞ

Denizcilikte güvenlik başlı başına mühim bir konu olmakla beraber siber güvenlik ise gelişen teknoloji ile beraber oldukça önem arz etmeye başlamıştır. Teknolojinin özel hayatımızda büyük yer kaplaması paralel olarak iş hayatımızda da yer almaktadır. Gemilerde kullanılan cep telefonu, bilgisayar veya kişisel teknolojik ekipmanlar ve bu cihazların gemi cihazlarıyla olan alışverişleri büyük bir siber güvenlik zafiyetine sebebiyet vermektedir.

Güvenlik konusunda ise yapılabilecek çeşitli önlemler ve yatırımlar olmakla beraber bu konuda en önemli payı eğitimli ve yetkin insan almaktadır. Güvenlik üzerine verilen açığın büyük bir bölümü insan temelli olmaktadır. Bu konuda personelin eğitimi ve farkındalık seviyesinin yükseltilmesi amacıyla eğitim ve yatırım şarttır. Kullanılan programlar ve donanımlar gelişen teknoloji ile beraber sürekli güncel tutulmalıdır. Şirketlerin siber güvenlik politikaları oluşan saldırı olayları ile beraber tekrar gözden geçirilip güncellenmesi önem arz etmektedir.

Bu çalışmada gemide kullanılan cihazların yapısının yanı sıra siber saldırılara karşı olan yetkinlikleri ve eksiklikleri detaylı olarak incelenmiştir. Bugüne kadar yapılan saldırılar incelenmiş ve bu saldırı şekillerinin analizleri yapılmıştır. Olası gemi siber atak senaryoları detaylı olarak incelenmiştir. Türk gemi işletmecileri bilişim departmanı yetkilileriyle görüşülerek analizler tamamlanmış ve konu ile alakalı önerilerde bulunulmuştur.

BİRİNCİ BÖLÜM
SİBER GÜVENLİK

1.1. DENİZCİLİKTE SİBER GÜVENLİK

1.1.1. Siber Güvenlik Tanım ve Kavramlar

Siber ataklar, zarar vermek, engellemek veya yetki dışı erişim sağlamak amacıyla yapılan atakların hepsine denmektedir. Siber güvenlik kavramı, bilgisayar ve bilgisayar sistemlerini atak ve izinsiz erişimlerden korumak için alınan önlemler olarak açıklanır (Merriamwebster, 2019).

Uluslararası Telekomünikasyon Birliği (International Telecommunication Union, ITU), siber güvenliği; "*Siber saldırılara karşı alınacak tedbirlerin bütünüdür. Kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullandığı araçlar, geliştirilen politika ve uygulamalar; yazılı belgeler, elektronik ortam dokümanları, etkinlikler, eğitimler ve bilişim alanında kullanılan güvenlik teknolojilerinin tamamı siber güvenliğin unsurları arasındadır.*" şeklinde tanımlamaktadır (ITU, 2008: 8-12).

Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve Eylem Planında ise, "*Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi*" şeklinde ifade edilmiştir (UDHB, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı: 47).

Tablo 1: Ulusal Siber Güvenlik İndeksi Sıralaması

SIRA	ÜLKE	ULUSAL SİBER GÜVENLİK İNDEKSİ	DİJİTAL GELİŞİM SEVİYESİ	FARK
1.	France	83.12	79.06	4.06
2.	Germany	83.12	81.95	1.17
3.	Estonia	81.82	79.27	2.55
4.	Slovakia	80.52	66.73	13.79
5.	Finland	79.22	82.26	-3.04
6.	Lithuania	77.92	70.95	6.97
7.	Spain	77.92	73.24	4.68
8.	United Kingdom	75.32	83.96	-8.64
9.	Switzerland	75.32	85.13	-9.81
10.	Czech Republic	74.03	69.37	4.66
11.	Malaysia	72.73	66.90	5.83
12.	Latvia	72.73	70.59	2.14
13.	Portugal	68.83	70.65	-1.82
14.	Belgium	68.83	77.62	-8.79
15.	Poland	67.53	66.59	0.94
16.	Serbia	66.23	61.62	4.61
44.	Turkey	45.45	61.83	-16.38

Kaynak: Ncsi, 2019.

Tablo 1'de ülkelere göre siber güvenlik indeksi sıralaması gösterilmektedir. İndeks ülkelerin dijital gelişim seviyesi ile ulusal siber güvenlik indeksi arasında fark oranı göz önüne alınarak yapılmış olup Türkiye -16,8 fark ile 44. sırada yer almaktadır.

Denizcilikte siber güvenlik ise liman, gemi ve bilgisayar destekli tüm denizcilik operasyonlarında kullanılan uygulama ve iletişim ağlarını korumak amacıyla alınan tüm önlemler olarak tanımlanabilmektedir. Otonom/yarı otonom gemi projelerinin artmasıyla denizcilik sektöründe teknolojinin payı giderek artmaktadır. Entegre köprüüstü ve dijital sistemlerin yaygınlaşması ile gemilerde ve limanlarda kullanılan yazılımlar artmıştır.

Günümüzde modern gemiler özellikle yolcu gemileri yüzen bilgisayarlar olarak tanımlanmaktadır, bu gemilerde kablosuz internet seçeneği okyanuslarda dahi sunulmaktadır. Gps ile yönetilen yükleme ekipmanları başta olmak üzere, komplex kargo operasyonları insansız ekipmanlar tarafından yönetilmektedir (Şakar ve Diğerleri, 2019: 6).

Dijital sistemlerin ve yazılımların güvenliği hem operasyonun emniyeti hem de barındırdığı ticari ve gizli bilgiler sebebiyle oldukça önem arz etmektedir. Siber saldırılara karşın güvenliğin sağlanması için alınacak siber güvenlik adımlarının güncelliği ve uygulanabilir olması şarttır. Önümüzdeki bu süreç içerisinde siber güvenlik uygulamalarının önemi teknolojinin gelişmesine paralel olarak daha fazla önem arz edecektir.

1.1.2. Siber Güvenlik Tarihçesi

Dünya e-devlet gelişim indeksine göre Estonya hükümeti yüzde 85 oranı ile ilk 20 de yer almaktadır. 27 Nisan 2007 ile 18 Mayıs 2007 tarihleri arasında 3 hafta süren ddos, dns, e-mail ve spam gibi çeşitli siber saldırılara uğramıştır. Estonya hükümeti bu saldırıların yeni seçilen hükümet ile Rus azınlıkları arasındaki çatışmadan doğduğuna ve dolayısıyla Rusya hükümetini sorumlu tutmuştur. Bu saldırı sadece hükümetler arası politikaları değil aynı zamanda siber güvenliğe bakış açısını ve internet kurulum tabanlarının tekrar yapılandırılması konusunda ışık tutmuştur (Schmidt, 2019).

Stuxnet solucanı ilk olarak 2010 yılı haziran ayında ortaya çıkmış, 500 kb boyutunda olup usb ile sisteme giriş sağlamıştır. 15 ten fazla İran nükleer tesisine sızmış olup en fazla tahribatı Natanz nükleer tesisine yapmıştır. İran'ın saldırıyla ilgili net açıklamalar yapmamasına rağmen stuxnet saldırısının 984 uranyum yapısını tahrip edip yüzde 30 oranında verimliliğin azalmasına sebep olduğu tahmin edilmektedir (Holloway, 2019).

Adobe firması Ekim 2013'te yaptığı açıklamada 2.9 milyon kişisel hesabın çalındığını (şifre, kullanıcı adı ve soyadı, kredi kartı numara ve son kullanma tarihi) ve 150 milyonun kullanıcın hesaplarının da bundan olumsuz etkilendiğini açıklamıştır. Aynı zamanda 40 gb kaynak kodu da sistemden çalınmış olup Adobe firmasını büyük zarara uğratmıştır (Outpost24, 2019).

Nisan 2011'de Sony Play Station siber saldırıya uğrayarak 77 milyon kullanıcı ve on binlercesinin banka hesap bilgileri ile beraber çalınmıştır. Bu olaydan sonra Sony Play Station şirketi bir ay süre ile kapalı kalmıştır. Çalınan hesaplardan kullanılan yasa dışı ücretler sebebiyle Sony firması 15 milyon dolarlık ödemeyi müşterilerine yapmıştır (Outpost24, 2019).

20 Mart 2013'te Güney Kore'de karanlık Seul olarak bilinen siber saldırılar ile birçok bankanın sistemini felce uğratmıştır. Medya tarafında da siber terör olarakta lanse edilen bu durum ülkede tüm bankacılık hizmetleri en az bir gün süre ile kesintiye uğratmıştır (Marpaung ve Lee, 2013: 3).

Marriot firmasının uğradığı siber saldırılar sonucunda 500 milyon kullanıcının kredi kartları dâhil tüm kişisel bilgileri çalınmıştır. Marriot bir Amerikan firması olmasına karşın müşterileri ağırlıklı olarak Avrupa vatandaşı olup bu durum şirketin yıllık gelirinin yüzde 4'ü oranında yani 900 milyon dolarlık bir ceza ile karşı karşıya bırakmıştır (Db Cyber Tech, 2019).

Ağustos 2014'te bilgi teknolojileri şirketi 'Hold Security' Rus hackerlar tarafından 1,2 milyar kullanıcı ve şifre bilgilerinin 420 bin website üzerinden çalındığını açıklamıştır. Bu durum 500 milyon kullanıcının mail hesabına erişim sağlamalarına olanak vermiştir. FBI bu durumun ciddi sonuçları olmadığını ve hackerların bu mailleri spam iletiler yolu ile sosyal iletişimler için kullandıklarını açıklamıştır (Outpost24, 2019).

Yahoo firması 2016 yılında, 2014 yılının sonuna doğru 500 milyon kullanıcının bilgilerinin çalındığını açıklamış ve bu olay internet tarihinin en büyük siber saldırılarından biri olarak tarihe geçmiştir (Theguardian, 2019).

1.1.3. Denizcilik Alanında Oluşan Olaylar

Uluslararası camiada birçok ambargo uygulanması sebebiyle denizcilik İran ekonomisinin canlı tutulmasında çok önemli bir rol oynamaktadır. Ağustos 2011'de IRISL devlet denizcilik şirketi siber saldırıya uğramıştır. Şirket genel müdürü Mohammad Hussein Dajmar'a göre; siber saldırı kargo bilgileri, genel şirket ve hat bilgileri de dâhil olmak üzere önemli bilgilerin çalınmasına sebebiyet vermiştir.

Çalınan bu bilgiler yüzünden konteyner gemilerinde ve rıhtımlarda yükleme ve tahliye sistemi çökmüştür (Reuters, 2019).

Ekim 2012'de ise başka bir siber saldırı daha gerçekleşmiştir. Bu sefer İran körfezinde yer alan gaz ve petrol platformlarıyla kurulan iletişim ağı hedef alınmıştır. Petrol İran ekonomisinde önemli bir yer almakta olup bu saldırı sonrası İran hükümeti ve yatırımcıları bu durumun petrol ticaretinde ekonomik krize sebebiyet vermesinden endişelenmişlerdir. Siber saldırılar ve tehditler İran'ı siber güvenlik alanında daha fazla yatırım yapıp siber güvenlik konusunda önlemler almaya yöneltmiştir (Maritimeexecutive, 2019).

Dünya petrolünün yüzde 10'nunu karşılayan devlet şirketi Saudi Aramco, bir personelinin oltalama (phishing) mailindeki bağlantıya (link) tıklamasıyla Ramazan ayında saldırıya uğramıştır. Önemli dosyalar silinmiş, telefon bağlantıları sağlanamamıştır. 35 bin bilgisayar çökertilmiş ve verilerin 4/3'ü sistemden silinmiştir. Bu atak yüzünden para transferleri yapılamamış, şirket içi iletişim çökmüş ve operasyon tamamen durma noktasına gelmiştir. Saldırıdan 14 gün sonra şirket olağan bir şekilde devlete petrol sağlamaya başlamıştır. Saldırı dünyanın en büyük petrol üreticisine ciddi hasarlar vermiştir (Middleton, 2012: 21).

Danimarka'da ise Nisan 2012'de siber saldırıya acente da çalışan bir kullanıcıya gönderilen mailin ekindeki virüs enfekte edilmiş pdf ile önce denizcilik otoritesinin tüm bilgisayarlarına ardından diğer devlet kurumlarına bulaştırılmıştır. Sonuç olarak Danimarka denizcilik otoritesi sistemini yeniden kurmak amacıyla, sistemi günlerce tamamen kapatmak zorunda kalıp yeni anti-virüs programlarını da yükleyip sistemi desteklemiştir. Saldırı sonrası sistem güvenliği ön planda tutularak çalışmalara devam edilmiştir (Maritimedenmark, 2019).

Avrupa'nın ve dünyanın en büyük limanlarından Antwerp (Belçika) limanı kaçakçılık maksadıyla 2013 yılının sonlarında siber saldırıya uğramıştır. Bir konteynerın limanda kaybolması ile siber saldırı anlaşılmıştır. Hacker'in virüsü kargo takip sistemine sızdırmasıyla terminal sistemine erişim sağlayarak olay vuku bulmuştur. Hacker uyuşturucunun saklı olduğu konteyneri sistem üzerinden tanıyıp liman ve şirket yetkilendirmesi gerekmeden tırlara yükleyip liman dışına tahliye edebilmektedir. Operasyon sonrasında konteyner bilgilerini de liman sisteminden silmiştir. Saldırı fark edilip konteyner yakalandığında 1044 kilo kokain, 1099 kilo

eroin ele geçirilmiştir. Hacker, konteynerin yüklendiği limanın ve tahliye limanın sistemini ele geçirerek konteynerin liman dışına çıkarıldıktan sonra her iki sistemden de bilgileri silmiştir (Bell, 2019).

Bu saldırı düşünüldüğünde dijital konteyner takibi ve dünyada konteynerleşme ile beraber olabilecek siber saldırılarının ne kadar ağır sonuçlar verebileceği ve siber güvenliğin ne kadar önemli olduğu görülmektedir.

Nisan 2016'da Güney Kore 280 geminin seyir sistemlerinde problem olduğunu raporlamıştır. Gps hackerler tarafından saldırıya uğrayarak sinyallerin yok edilmesine ve yanlış bilgi vermesine sebebiyet vermiştir. Gps sinyallerinin yanıltması veya kaybolması bir sürü seyirsel hataya aynı zamanda trafiğin sıkışık ve hava koşullarının ağır olduğu yerlerde ciddi kazalara sebebiyet verebilmektedir.

Şubat 2017'de 8250 teu'luk konteyner gemisi Kıbrıs'tan Djıbutı'ye seyrederken siber saldırıya uğrayarak tüm seyir sistemi ele geçirilmiştir. 10 saat süreyle tüm seyir sistemi ele geçirilmiş ve kaptan hiçbir şekilde bu duruma müdahale edememiştir. Siber korsanların amacı geminin tüm kontrollerini ele geçirerek istedikleri bölgeye seyretmesini sağlamak idi. Şirketin bilişim uzmanlarının gemiye çıkıp müdahale etmesiyle tekrar kontrol geri alınmış ve siber saldırılara karşı daha etkin yeni güvenlik programı yüklenmiştir (Silgado, 2018: 44).

Haziran 2017'de A.P Moller-Maersk şirketi notpetya adı verilen siber saldırı kurbanı olmuştur. 600'den fazla konteyner gemisi ve markette yüzde 16'lık pay ile dünyanın en büyük denizcilik şirketleri arasında yer alan şirket Asya-Avrupa hattında yüzde 25'lik bir pay ile taşımacılık yapmaktadır. Maersk yöneticisi Jim Hagemann Snabe Ocak 2018 dünya ekonomik forumunda yaptığı açıklamaya göre;

> *''Maersk bilişim sistemindeki saldırının ardından konteyner taşımacılığı, liman operasyonları, petrol, gaz platformları ve petrol tankerleri de dâhil olmak üzere tüm işletmeleri kötü etkilendi. Siber saldırının yüksek etkisine rağmen filo ve tüm denizciler tehlike altında olmayıp Maersk bu süre içerisinde bütün operasyonlarını manuel olarak devam ettirmektedir.''*

Maersk notpetya adı verilen fidye yazılım (ransomware) kurbanı olmuştur. Malware saldırı ile tüm sisteme yayılan virüs ekranda dijital para (bitcoin) aracılığı ile fidye isteyen bir form belirtmektedir (Lagouvardou, 2018: 90).

Bu saldırı Maersk firmasını 10 gün süre ile tüm sistemini kapatmasına sebebiyet vermiştir. Bu süreç içerisinde 40.000 server, 25.000 bilgisayar, 2500 uygulamayı sisteme tekrar yüklemeye çalışmıştır. Maersk yöneticisi Jim Hagemann Snabe'ye göre; tüm işlerin tekrar prosedürlere uygun yürümesi en az 6 aylık bir süre alacağını ve saldırının 200 ile 300 milyon dolarlık bir zarar verdiğini belirtmiştir (Investormaersk, 2019).

Cosco Denizciliğin sahibi olduğu Cosco Long Beach Terminali siber saldırılara maruz kalmıştır. Ataklar firmanın operasyonlarını etkilememesine rağmen firma güvenlik amacıyla kısa bir süreliğine diğer tüm bölgelerle iletişimi kesip sistemi kapatmıştır. Sistem tekrar açıldığında tüm müşterilerine her şeyin güvende olduğunu ve operasyona devam edildiğini açıklayan bir mail ile bilgilendirmiştir (Tradewinds, 2018: 24).

20 Eylül 2018'de Barcelona limanı siber saldırıya uğradığını Twitter aracılığı ile açıklamıştır. Operasyonlar bu saldırıdan liman otoritesinin acil eylem planları sayesinde etkilenmemiştir. İlginç olan ise saldırıdan sadece iki gün önce limanın resmi Twitter sayfasından 'Hiçkimse, limanlar da dâhil olmak üzere siber saldırılara karşı emniyetli değil ve bu durum tüm şirketleri ve paydaşlarını risk altında tutuyor, siber güvenlik sistemlerini liman üzerinde uyguluyoruz' şeklinde bir açıklamada bulunmuştur (Securelist, 2018).

1.2.SİBER SALDIRI ÇEŞİTLERİ

1.2.1. Kötülümcül Yazılım (Malware)

Kötülümcül yazılımın İngilizce kısaltması olan malware (malicious software) kullanıcının veya ağın bilgisi dışında sisteme ve bilgisayara erişmek veya zarar vermek üzere yaratılmış bir yazılım türü olarak tanımlanmaktadır. İnternet dünyasında birçok tehdit bu terim altında tanımlanabilir.

Kodlama ile yazılımlar yazıp tüm güvenlik duvarlarını aşabilen siber korsanlar bilgisayarlara ve iletişim ağlarına zarar verebilir. Bu saldırıların temel

amacı bilgi kaynağını çalmak veya iletişim ağlarına zarar vermektir. Bu saldırı tipleri arasında virüs, truva atı, solucanlar veya casus/fidye amaçlı yazılımlar sayılabilir (Lagouvardou, 2018: 45). Aşağıda bu saldırı tiplerinin kısaca açıklamaları yapılmıştır.

Virüs: Biyolojik virüslerden esinlenerek adlandırılan ve bilgisayarla kolayca yapılan tehlikeli bir türdür. İnternet, email, usb/flaş tarzı harici ekipmanlar ile sisteme bulaşır. Makro, betik, ön yükleme ve dosya virüsleri olmak üzere dörde ayrılır (Canbek ve Sağıroğlu, 2006).

1948 yılında John Von Neuman tarafından ortaya atılmış olup ilk olarak kendisini kopyalayabilen bilgisayar programlarıdır. 1982'de ise Rick Skrenta çalışan ilk virüsü Elk Cloner ismiyle yazmıştır. Apple DOS 3.3 işletim sistemine disketler aracılığı ile bulaşmıştır. Lise öğrencisi olan Rick Skrenta tarafından arkadaşlarına şaka maksadıyla hazırlanmış olan bu program kendini oyun dosyaları içerisinde gizlemekte ve her açıldığında kızdırmak amaçlı bir şiir olarak ekrana gelmekteydi (Demirer, 2009).

Virüs kötülümcül yazılımların giderek yayılması teknolojini gelişmesi ile beraber ciddi bir tehdit haline gelmiştir. Bu durum virüs karşıtı (anti-virüs) veya güvenlik duvarları programlarının yaygınlaşmasına sebep olmuştur.

Truva Atı (Trojan Horse): Yunan mitolojisindeki truvadan esinlenerek yaratılmıştır. Program içerisine eklenen tehlikeli kodlar ile kullanıcının talimatları dışında işlem yapıp zarar verebilir (Gürsoy, 2015: 81). Arka kapı açarak bilgisayarları uzaktan yönetir. Yasa dışı siteler, müzik veya oyun sitelerini ziyaret esnasında program indirirken istemsiz olarak kötü niyetli programlarda indirilir.

Kurulumdan sonra arka plandan çalışıp korsana uzaktan erişim sağlar. Sisteme arka kapıdan (backdoor) erişen korsanlar, kişisel bilgilere, şifrelere ve sistemin yapısına kolayca erişebilir. Sisteme bulaşan Truva atı, belleğe yüklenip sistem açıkları dahilinde korsanın tüm talimatlarını yerine getirmektedir (Değirmenci, 2002: 63).

Solucanlar (Worms): Bilgisayar ağları arasında bir etkileşime ihtiyaç duymadan kendi kendine çoğalabilen ve herhangi bir programa ihtiyaç duymadan zarar verebilen kötülümcül yazılım türüdür. Solucanlar bilgisayara mail (spam) veya anlık mesajlara (ıms) tıklanarak bulaşır ve otomatik olarak bilgisayara yüklenir ve

gizlenirler. Solucanlar dosyaları değiştirebilir, silebilir ve farklı yazılımları yükleyebilir. Bazı solucanları ise durmadan çoğalarak sistem kaynaklarını tüketir, (harici disk boş alanlar) ağır işleyiş ve çöküşlere sebebiyet verebilir. Aynı zamanda sistemden bilgi çalıp transfer edebilir ve korsanın bilgisayara erişimini sağlayabilir (Usnorton, 2019). "John Brunner tarafından 1975 yılında yazılan "Shockwave Rider" isimli romanda, ağ üzerinden yayılabilen programa verdiği isimden gelmektedir" (Canbek ve Sağıroğlu, 2006).

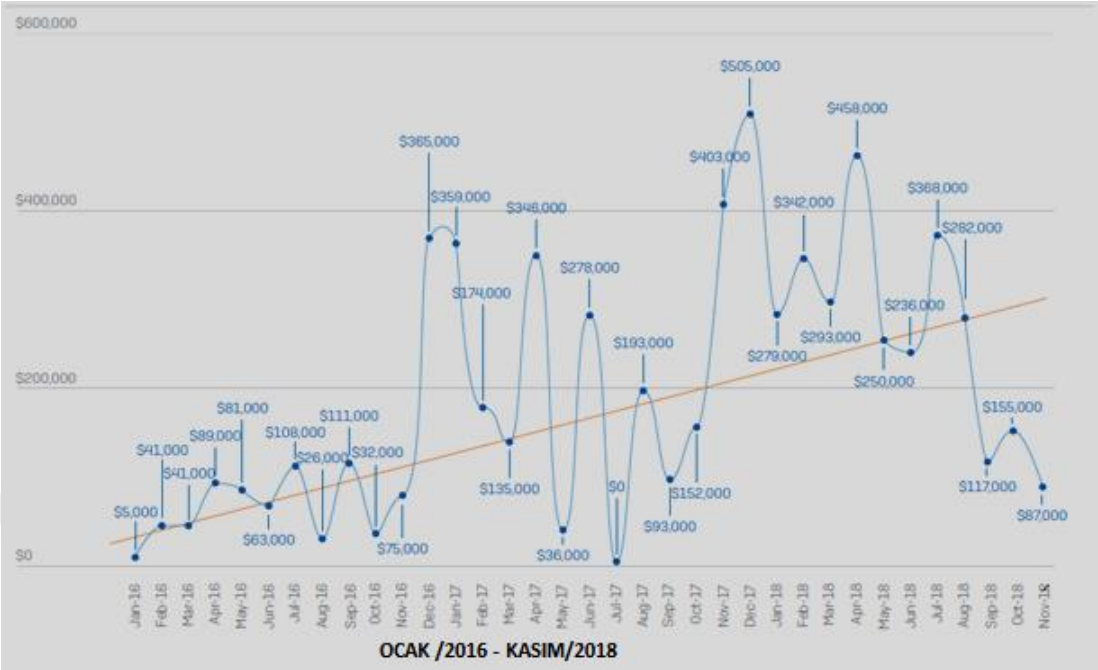
Arpanet ağına yüklenen program ile tarihte ilk solucan olayı ABD'de 2 Kasım 1988'de görülmüştür. Yazılım hızlıca yayılarak bilim ve askeri sistemlerine bulaşmıştır. 2000 bilgisayar bu durumdan kötü etkilenerek yaklaşık 150.000 dolar zarar verilmiştir (Dülger, 2004: 212). 2010 yılında stuxnet adlı solucanın İran nükleer tesisine sızarak verdiği zararı da kısaca siber güvenlik tarihçesi kısmında da özetlemiştik.

Casus Yazılım (Spyware): Bilgisayara sızdıktan sonra kullanıcın bilgi dışında 3.kişilere bilgi, şifre, kredi kartı bilgileri, internette sık ziyaret edilen sayfalar gibi önemli kişisel bilgileri aktaran yazılımlardır. Bu aktivitelerin hepsi sistem hızında ve ağlarda yavaşlamaya sebebiyet vermektedir. Günümüzde internete bağlı her bilgisayara bulaşıp ciddi zararlar veren bir yazılım olup bu konuda tedbirli olmak oldukça önemlidir (Kaspersky, 2019).

Fidye Yazılım (Ransomware): Bu yazılım sızdığı bilgisayarı kilitleyip şifreliyor ve ardından kullanıcının tekrar erişim sağlamasına izin vermek için de fidye talep etmektedir. Aynı zamanda yapılan ödemenin ardından tüm bilgileri sağlam bir şekilde geri alınacağının da garantisi yoktur. Genelde online oyunlar üzerinden bilgisayara bulaşmaktadır. Çeşitli saldırı tipleri olmakla beraber günümüzde oldukça aktif bir şekilde kullanılmaktadır. Dolaysıyla kurban olmadan önce güvenlik önemleri almak önemli bir yer tutmaktadır (Usnorton, 2019).

Tablo 2'ye göre yapılan saldırılar temmuz ayında en düşük seviyeleri görürken kasım ayında zirveye ulaşmış ve oluşan maddi zarar oldukça yüksek seviyelere ulaşmıştır.

Tablo 2: Saldırı Raporu



Kaynakça: Sophoslabs, 2019.

Tablo 2'de fidye yazılım korsanlığından toplamda 6 milyon dolar dolandırıcılık yapılmış olduğu ve günden güne bu miktarın artış gösterdiği anlaşılmaktadır.

Tablo 3: Sistem Tehdit Raporu

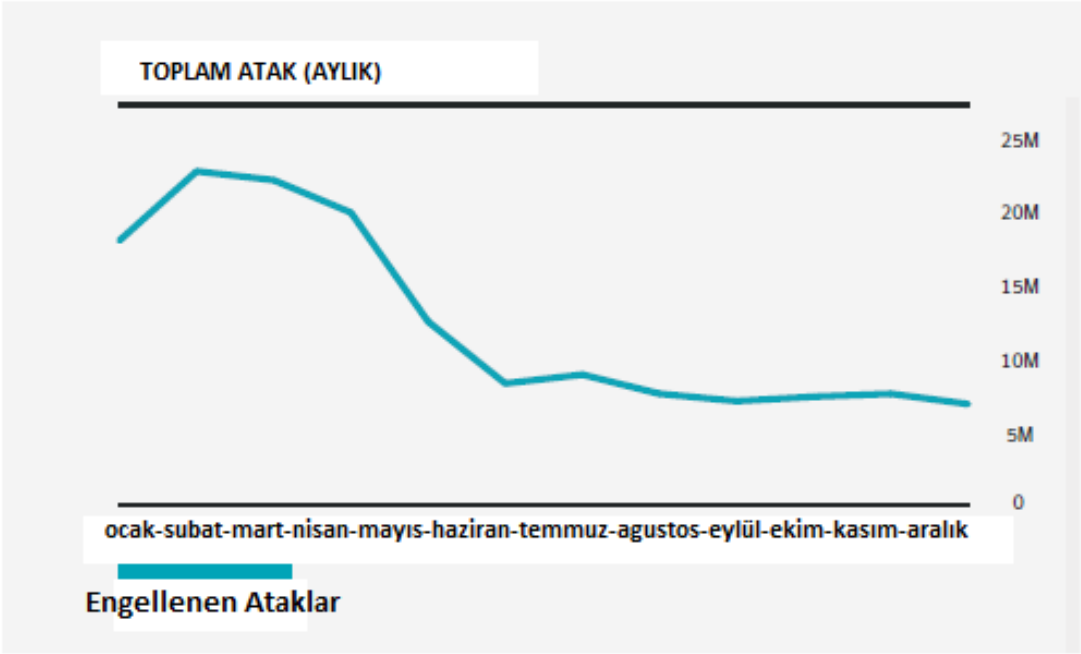
YILLIK BAZDA SİSTEM ATAKLARI

YIL	SİSTEM	ENGELLENEN ATAKLAR	ORAN
2016	Windows	161,708,289	98.5
	Mac	2,445,414	1.5
2017	Windows	165,639,264	97.6
	Mac	4,011,252	2.4
2018	Windows	144,338,341	97.2
	Mac	4,206,986	2.8

Kaynakça: Symantec, 2019.

Tablo 3 ise yıllık bazda yapılan ataklara karşılık olan engel sayısı ve oranını göstermektedir. Windows sisteminde bu oran yüzde 97.2 lerde iken Mac sisteminde bu durum yüzde 2.8 civarındadır. 2018 yılında Windows sistemi Mac sistemine göre azalma gözükse de oranının büyük kısmı yine Windows sistemine aittir.

Tablo 4: Aylık Atak Raporu



Kaynakça: Symantec, 2019.

Tablo 4'te ise aylık bazda yapılan atakların grafiği çizilmiştir. Şubat aylarında bu durum zirvedeyken haziran ayı ve sonrası için azalma eğilimindedir.

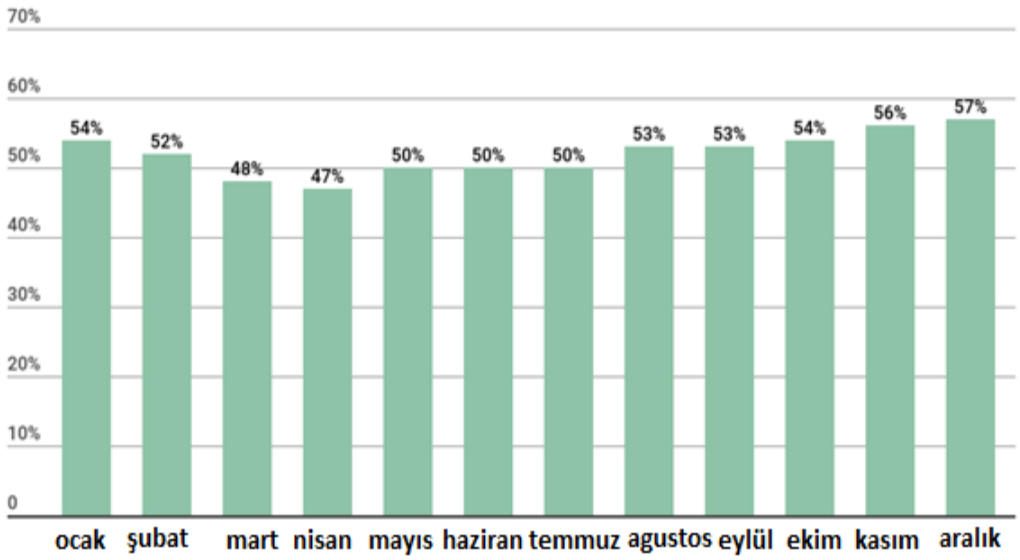
1.2.2. Oltalama (Phishing)

Oltalama (yemleme) saldırıları genelde kurbana sahte bağlantı (link) içeren elektronik postalar gönderme yöntemi olarak kullanılır. Gelen bu posta genellikle banka, resmi kurumlar ve benzeri yerlerden gelmiş gibi gözükerek linke tıklanması durumunda tüm kişisel ve diğer önemli bilgiler saldırgan tarafından ele geçirilir. Bu tip saldırılardan korunmanın en iyi yolu ise oltalama email konusunda kullanıcının eğitimli olması ve bağlantılara tıklamadan kaçınmasıdır (Pajunen, 2017; 21).

Oltalama saldırıları internet saldırıları arasında en yaygın ve en tehlikeli olanlarındandır. İngilizce balık tutma anlamına gelen ‘fishing’ sözcüğündeki ‘f ’ yerine ‘ ph ’ harflerini konulmasıyla türetilen terim, attığımız zaman en azından bir balık yakalayabileceğimiz düşüncesinden esinlenerek oluşturulmuştur (Turhan, 2006 :57).

İstenmeyen E-Posta (Spam): İngilizce kelime olan ‘spiced pork and ham’ baharatlı domuz eti ve jambon anlamına gelip baş harflerinin birleştirilmesiyle oluşturulmuştur. Pazarlama, reklam veya sosyal içerikli olarak büyük kitlelere ulaştırılmak istenen mesajların kullanıcının isteği dışında kendisine yollanmasına dayanmaktadır (Turhan, 2006: 58).

Tablo 5: Spam Oranı



Kaynakça: Kaspersky, 2019.

Tablo 5’e göre e-mail iletilerinde spam iletilerinin payı Nisan ayında en düşük seviyelerde iken aralık ayında en yüksek seviyelere ulaşmaktadır.

1.2.3. Su Kaynağı Saldırısı (Watering Hole)

Su kaynağı saldırısı; yapılacak şirket veya kurum tarafından sıklıkla ziyaret edilen web siteleri tespit edilip, bunlardan biri veya daha fazlasına kötülümcül yazılımların veya zararlı kodların yerleştirilmesi ardından bu web sitelerine girilmesi neticesinde bu kötülümcül yazılımların sisteme bulaştırılması yoluyla yapılmaktadır (Yaşar ve Çakır, 2015: 8). Bu saldırı türü diğer saldırılara göre daha stratejik ve hedef odaklıdır. Rastgele sitelere veya maillere erişmeye çalışmak yerine belli bir gruba erişmeye çalışıldığından, o grubun güvenli sanacağı, kanacağı yollara başvurulur ve başarı oranı yüksektir (Solidthink, 2019).

1.2.4. Hizmet Engelleme Saldırısı (Dos)

Hedef sistemin erişilebilirliğini engellemek için yapılan, bilişim sistemleri hakkında çok fazla teknik bilgiye sahip olunmasını gerektirmeyen saldırı çeşididir. Akşam trafiğinde trafiğin kilitlenerek durması DOS atak saldırısının çalışma yapısına benzetilebilir. Eğer yolun kapasitesinin üstünde araç bulunursa yollar tıkanır. Sistemin bant genişliğini aşacak şekilde paketlerin yollanmasıyla sistemin erişilebilirliği engellenir. Eğer gelen trafiğin bant genişliği saldırı alan sistemin bant genişliğinden daha fazla ise yapacak bir şey yoktur (Akyıldız, 2013: 36).

T.C. Ölçme, Seçme ve Yerleştirme Merkezinin resmi web sitesi olan www.osym.gov.tr'ye, sonuçların açıklandığı dönem erişim pek sağlanamamaktadır. Buradaki hizmet milyonlarca kişinin aynı anda siteye erişmek istemesiyle hizmet sağlanamamaktadır (Başar, 2015: 34).

1.2.5. Botnet Saldırısı

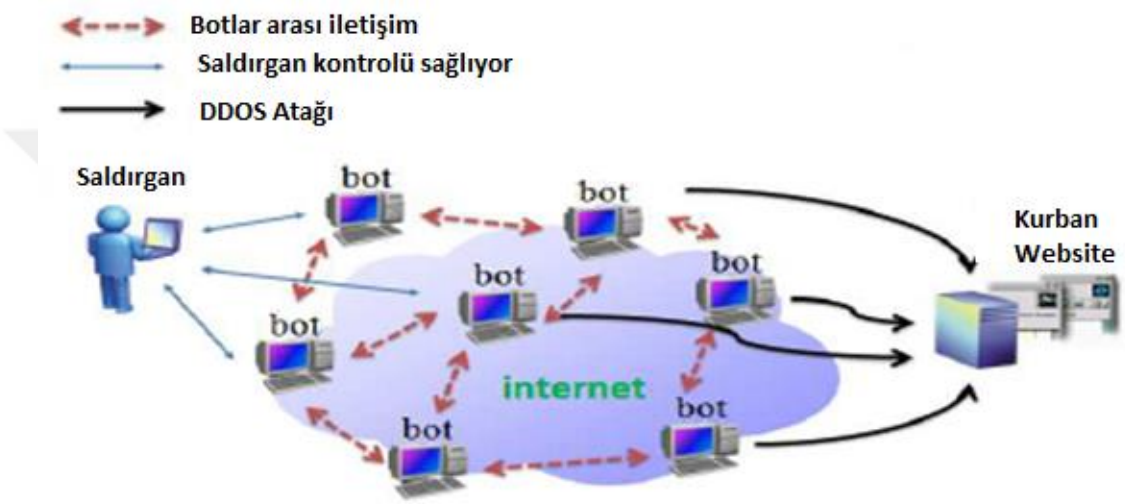
"Robot" sözcüğü ile anlamlandırılan "BOT", belirli bir görevi bir insandan daha hızlı gerçekleştiren ve tekrar eden bir uygulamadır. "BOTNET" ise, ağ yardımıyla birbirine bağlı birkaç BOT'un bir arada kullanılmasıdır. BOTNET saldırısının üç temel unsuru; Bot, Komuta ve Kontrol (C&C) Sunucusu ve Botmaster'dır (Dergipark, 2019).

Kötülümcül yazılım olup bilgisayara bulaşan botlar, botmaster tarafından komuta edilip spam mailler, önemli bilgiler, şifreleri karşı tarafa gönderebilir.

Bunlara ek olarak rutin işleyişi de bozup kalıcı hasarlara sebebiyet verip ağları veya bilgisayarları kullanım dışı bırakarak ciddi ekonomik ve politik zararlar verebilir (Unibonn, 2019).

Şekil 1'de botlar arası iletişim saldırgan ve ddos atağı temsili olarak gösterilmiştir.

Şekil 1: Botnet Saldırı



Kaynakça: Abdullah ve Diğerleri, 2019.

1.2.6. Ortadaki Adam Saldırısı (Man In The Middle)

Siber varlıklar iletişim kurabilmek amacıyla veri gönderme ve almak için çeşitli ağlarla bağlantı kurmaktadır. Kurulan iletişimlerin korsanlar tarafından manipüle edilmesine ortadaki adam saldırısı olarak tanımlanmaktadır (Bozgeyik, 2018: 54). Bu yöntem kurbanın bu durumdan haberi dahi olmadan bütün dijital verilerin çalınmasına sebebiyet verir.

1.2.7. Dns Saldırısı (Pharming)

Erişilmek istenen internet sayfası dışında başka bir sayfaya yönlendirilmesi metoduna dayanan saldırı tipidir. IP adresleri alan adı sunucusu (DNS) tarafından çözümlenmekte ve çözümlenme aşamasına korsanlar tarafından müdahale edilmektedir. DNS sunucusu veri tabanı olan bilgisayar sunucu olup, site ismini girilmek istenen sitenin IP adresine yönlendirir. İnternet adreslerinin listelendiği 'host' olarak adlandırılan veriye yazılımlar vasıtasıyla erişen korsanlar, bankasının web sitesine erişmek isteyen kullanıcıyı, doğru web adresi yazmasına rağmen yanlış adrese yönlendirmektedir. Bu yolla kullanıcının internet bankacılığına dair kullanmış olduğu tüm kişisel verileri korsanlar tarafından elde edilmektedir (Gürsoy, 2015: 99).

1.2.8. IP Aldatması (IP Spoofing)

Bilgisayara izinsiz bir şekilde erişim sağlayan saldırı türüdür. Saldırgan kullanıcı güvenilir bir IP den imiş gibi mesaj gönderir. Bu mesajın ardından saldırgan kullanıcın IP adresini ele geçirir ve internet üzerinden farklı paketler göndererek bilgi alışverişine başlar. Bu alışverişin ardından IP adresini değiştirerek güvenilir bir adres gibi gösterir. IP aldatması olarak bilinen bu aşamanın ardından saldırgan saldırılarına başlamaktadır (Abdul-Mumın, 2011: 31).

1.2.9. İnsan Faktörü (Sosyal Mühendislik)

Bilişim sistemleri günden güne gelişimini sürdürmekte güvenlik açısından her türlü açığı kapatmaya çalışmaktadır. Bunlara güvenlik duvarları, anti virüs ve koruma programlarını örnek verebiliriz. Her ne kadar gelişim sağlansa da en zayıf halka olarak insanın yer alması kaçınılmaz hataların yapılmasına ve güvenlik duvarlarının aşılmasına sebebiyet vermektedir. Sosyal mühendislik saldırganlar için en iyi saldırı biçimlerindendir. Her atak için bazı araç, gereçler ve sınırlamalar mevcut iken sosyal mühendislikte bunların hiçbirine ihtiyaç duymayıp sınır tanımayan bir saldırı tipidir.

Saldırgan kurbana psikolojik yönden saldırıp ele geçirdiği için kişi ile alakalı tüm bilgileri ele geçirebilir. Sosyal mühendislik saldırı tipleri sahte email ve telefon konuşmaları ile dahi yapılabilen dolayısıyla pek teknik bilgiye ihtiyaç duyulmayan saldırılardır (Maan ve Sharma, 2012: 557).

Sosyal mühendislik, insanların güven eğilimlerini manipüle edip kurban eden saldırı biçimidir. Gelişmiş güvenli bilişim sistemleri dahi kurbanları bu saldırılardan koruyamamaktadır. İnsanlar kolayca saldırıya uğramakta ve yaptıkları riskli sosyal medya paylaşımları ile kendilerini kolayca hedefe koymaktadırlar. Güvenli olmayan internet sayfalarında gezinti yaparak, zararlı bağlantılara tıklayıp yüklenen kötülümcül yazılımlar sayesinde kullanıcı bilgisayarı kolayca enfekte olmaktadır (Conteh ve Scmick, 2016: 31).

Yukarda da saldırı tiplerinden bahsettiğimiz tüm siber saldırıların temelinde sosyal mühendislik yatmaktadır. İnsanları bir şekilde manipüle edip ele geçirilen bilgiler veya kontrollerle kurum veya şahıslara ciddi zararlar verilmektedir. Bu konuda farkındalığın artırılması ve eğitimlerin düzenlenmesi bu saldırıların önüne geçebilmek adına alınabilecek en önemli adımlardandır.

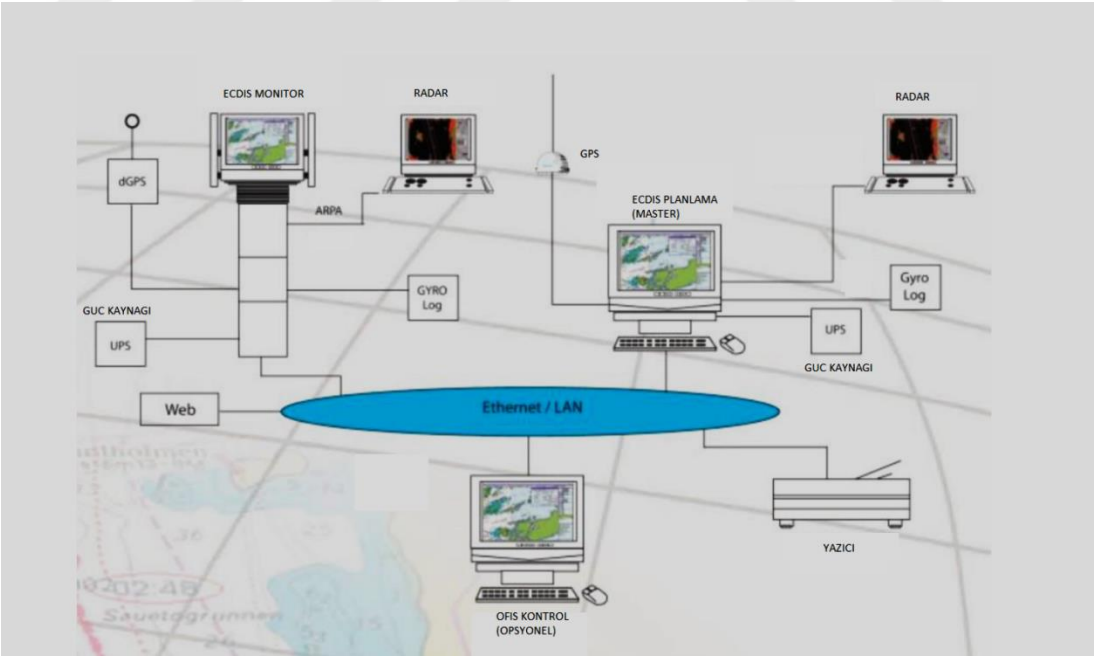
İKİNCİ BÖLÜM
SİBER SALDIRIYA UĞRAYABİLECEK KÖPRÜSTÜ CİHAZLARININ YAPISI

2.1. ECDIS

Elektronik harita ve gösterme sistemi (Electronic Chart And Display System) kısaltması olarak kullanılır. Ecdis bilgisayar temelli seyir haritası ve bilgi sistemidir. Geleneksel kâğıt haritalara alternatif olarak kullanılmaktadır. IMO'nun kurallarına göre ise, günümüzde tüm ticari gemilerde Ecdis bulunma zorunluluğu vardır (Nccgroup, 2014: 3).

Bilgisayar temelli ve sürekli güncelleme alan bir sistem olduğundan dışardan gelebilecek siber saldırılara açık ve olabilecek saldırılar sonucunda da ağır sonuçlar doğurabilecek bu sistemde güvenlik oldukça önemli yer kaplamaktadır. Ecdis bağlantı sistemi basit temelde ise Şekil 2'deki gibidir.

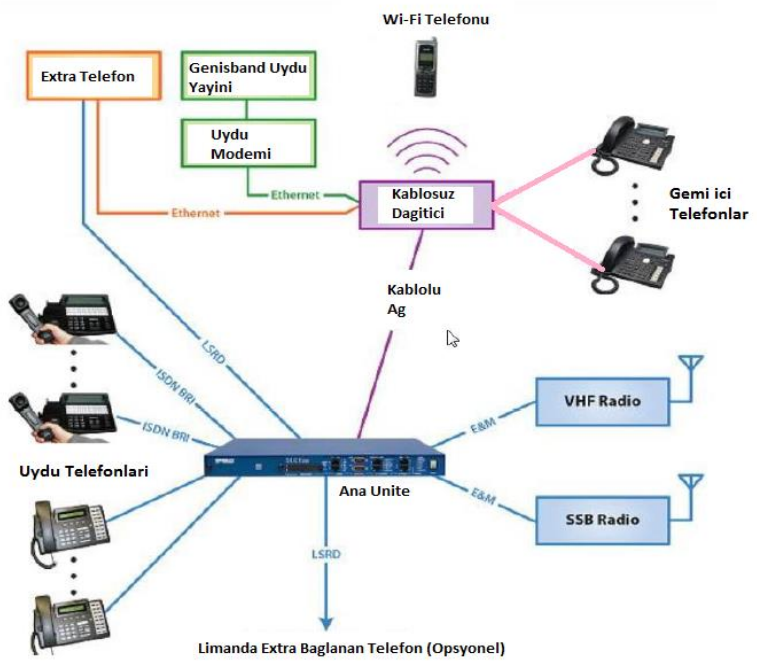
Şekil 2: Ecdis Ağ Sistemi



Kaynak: Nautico, 2019.

Ethernet/ Lan olarak gösterilen kısımda ise bağlantı sistemi temel olarak Şekil 3'te gösterildiği gibidir.

Şekil 3: Ethernet/ Lan Sistemi



Kaynak: Redcom, 2019.

Yukardaki grafiklerde de görüldüğü gibi uydu, telefonlar, Gps, Ais, Navtex ve diğer cihazlar Ecdis ile ortak ana üniteye bağlıdır. Bu ortak ünitede internet erişimini sağlamakta ve dağıtılmaktadır. Düzeltme gelen veya güncellenen Ecdis haritaları internet üzerinden indirilmekte veya usb/cd üzerinden aktarılarak Ecdis güncellenmektedir. Bu durum Ecdis cihazını siber saldırılara karşı açık hedef konumuna getirmektedir. Güncellemelerde kullanılan usb/cd veya internet üzerinden erişim sağlanarak ciddi mali ve çevre zararlarına, kazalara, gemi şirket bilgilerin çalınmasına sebebiyet verebilir.

Siber güvenlik açısından en önemli hususlardan biri de bağlantı hızının gelişen teknoloji ile beraber 50 mbps ye kadar yükselmesi denizlerde ucuz ve hızlı bağlantıların olmasına olanak sağlamasıdır. Hızlı bağlantı sistemleri gemileri siber güvenlik açısından daha kırılgan bir yapıya sokmaktadır.

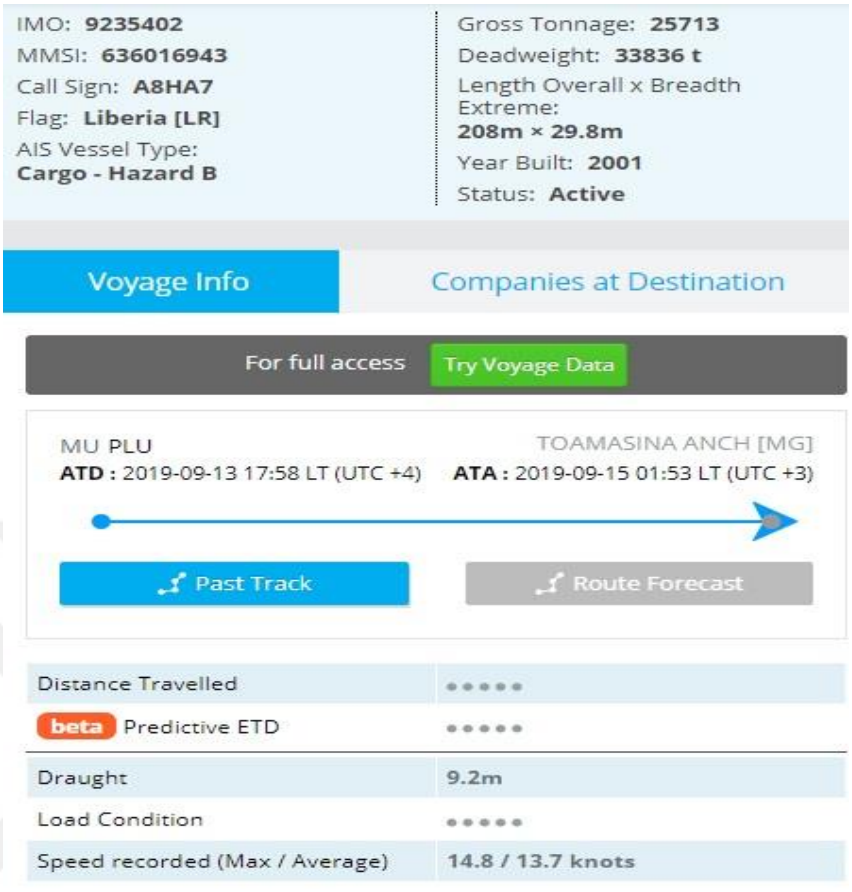
Denizcilikte artan saldırılara karşın UKHO (United Kingdom Hydrographic Office) ENC (Elektronik seyir haritaları) dağıtım standartı kurmuş ve bununla alakalı bilgi güvenlik standartları (S-63) yayınlanmıştır. Dünyadaki bütün tedarikçiler bu standartlara uymak zorundadır. Bu standartlar aynı zamanda AVCS (Admiralty Vector Chart Service) tarafından da uygulanmaktadır.

S-63 bir standart kriptografik sistemi olup hidrografik ofislere ve Ecdis üreticilerine Enc ve verilerine koruyabilecekleri güvenlik araçları sağlar. Bu güvenlik araçları ve uygulamaları Ecdis ve haritaların güvenliğini artırmaktadır (Admiralty, 2019).

2.2. AIS

Automatic Identification System açılımının kısaltması olarak kullanılan Ais, otomatik tanımlama sistemi olarak Türkçeye çevrilir. Ais bir gemi trafik takip sistemi olup çevredeki Ais tanımlı gemi trafiğinin diğer gemiler tarafından takip edilebilmesini sağlar. Ais tanımlı gemilerde gemi adı, Imo numarası, bağlama limanı, geminin boyutları, pozisyon bilgileri, rota, kerteriz, varış noktası, durumu ve diğer bilgiler görüntülenebilir. Web siteleri de Ais'ten topladığı bilgilerle veri merkezi oluşturup yakın gemilerin karadaki sistemler tarafından takip edilip bilgi alınmasını sağlamaktadır. Şekil 4 ve 5'te marinetraffic.com sitesinden alınan bilgi ekranı gösterilmiştir.

Şekil 4: Web Tabanlı Bilgi Sistemi



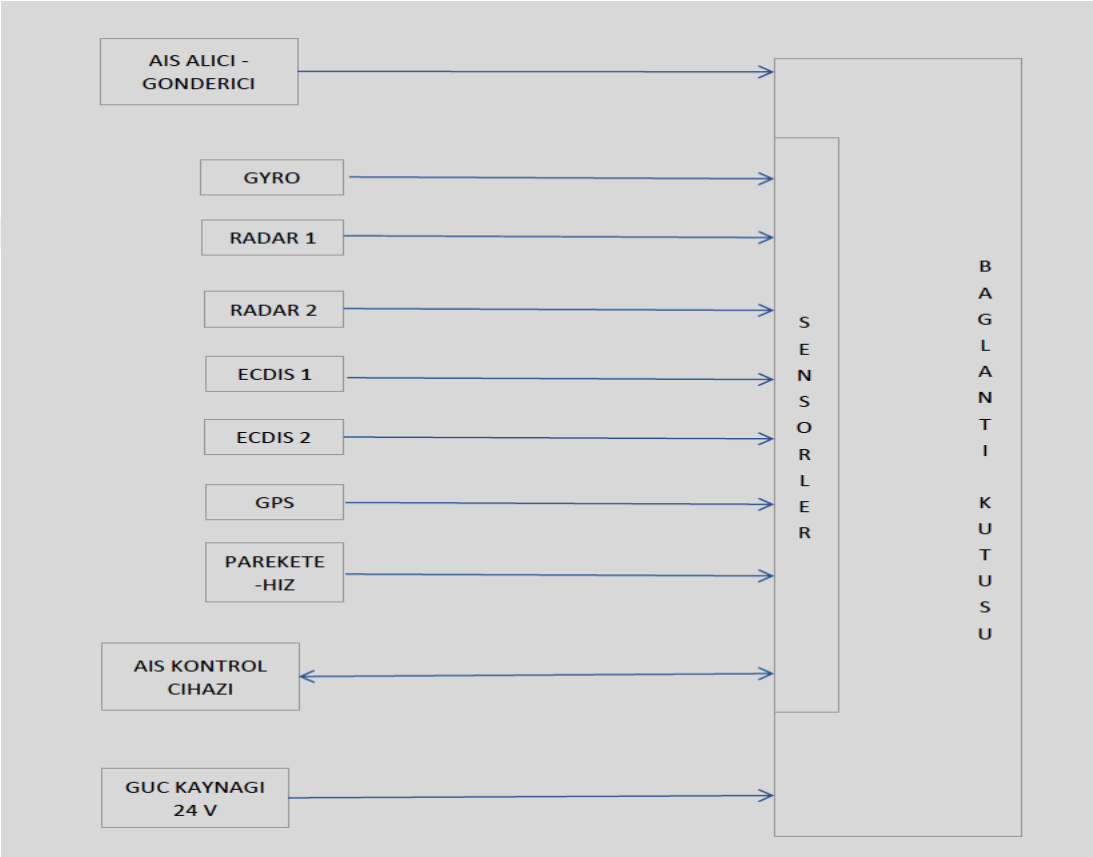
Kaynak: Marinetraffic, 2019.

Şekil 5: Web Tabanlı Detay Bilgi Sistemi

Kaynak: Marinetraffic, 2019.

Ais cihazı köprüüstündeki cihazlarla entegre durumda olup seyir yardımcı cihazlarındandır. Örnek olarak Jrc Ais ekipmanının köprüüstü cihazlarıyla entegre sistemi Şekil 6'da ki gibidir. Şekilde de görüldüğü gibi gemideki tüm iletişim cihazları entegre sistem halindedir.

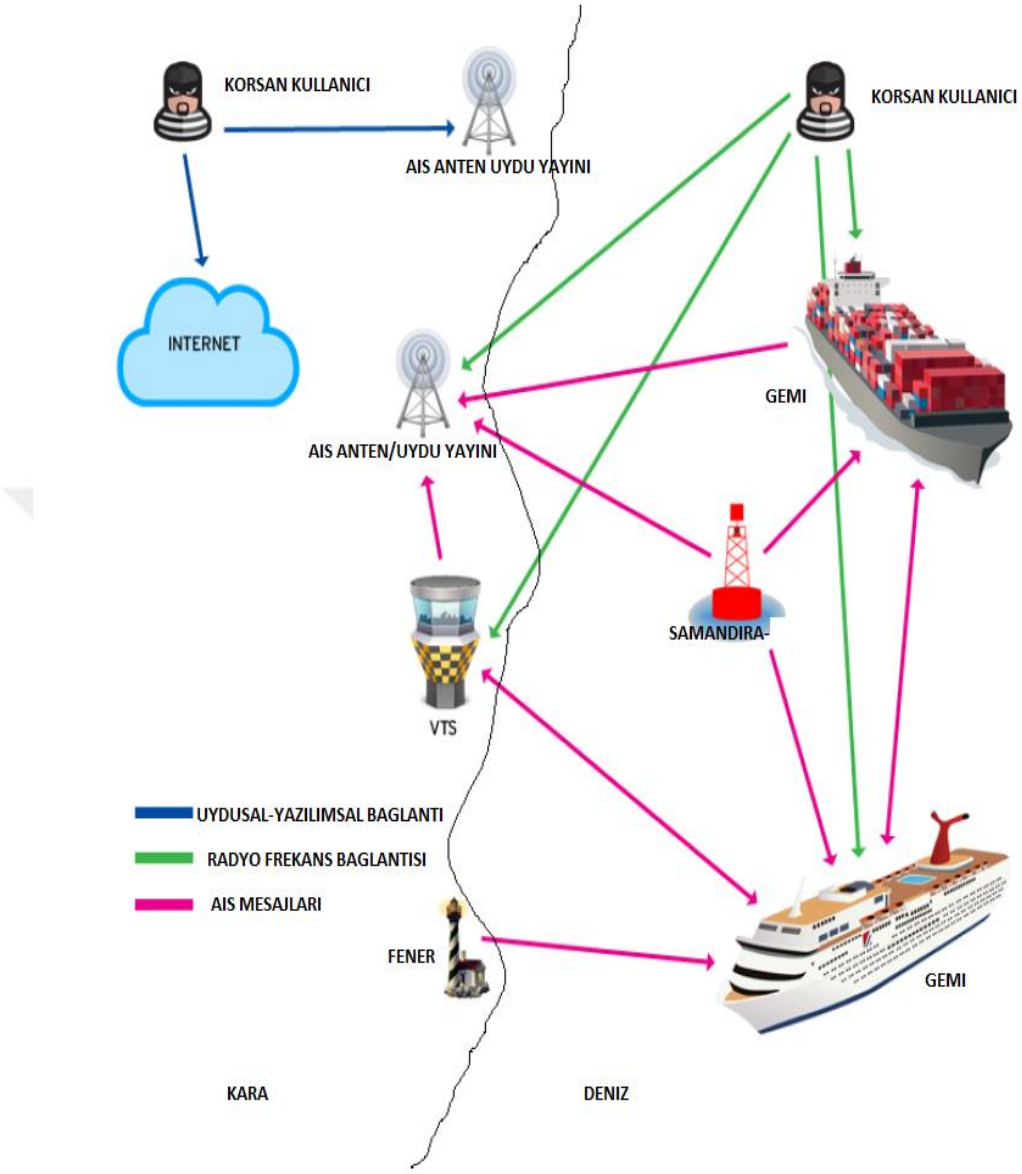
Şekil 6: JRC Ais Blok Şeması



Kaynak: Jrc, 2004.

Yeni nesil gemilerin neredeyse tamamında Ais bilgisi Radar Ecdis ve Gps sistemine entegre bir şekilde yansır ve operasyonel açıdan kullanıcıya kolaylık sağlar. Şekil 6 ise entegre sistemi açık bir şekilde göstermektedir. Ais cihazının muhtemel saldırı yapabilecek korsan kullanıcının da yer aldığı bilgi iletişim sistemi Şekil 7'deki gibidir.

Şekil 7: Ais İletişim Diyagramı



Kaynak: Balduzzi ve Wilhoit, 2014: 4.

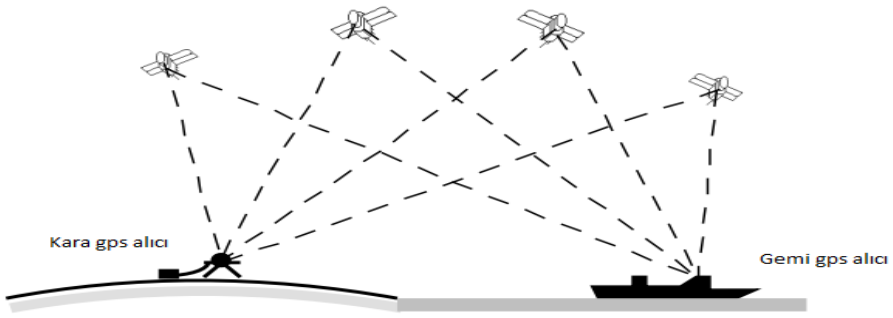
AIS bilgileri, cihaza ve anlık duruma bağlı olarak düzenli aralıklarla yayınlanır. Class B Ais ile donatılmış gemilerde 23 knot ve üstü yol yaptığı zamanlarda 5 saniyede bir yayın yapmakta iken, bir şamandıra veya fener herhangi bir tehlike yayını ise 3 dakikada bir yapmaktadır.

2.3. Gps

Global Positioning System kısaltması olarak tanımlanan Gps Amerikan ordusu tarafından kullanıma başlanmış hemen ardından neredeyse tüm sivil alanlarda kullanılmaya başlanmıştır. Askeri alanda kullanılan gps aksine sivil alanda kullanılan gps sisteminde güvenlik veya emniyet tabanlı kodlama/şifreleme veya uygulamalar yeterli seviyede değildir. Gps sistemi anlık mevkiimizi sağlamakla beraber gündelik hayatta da araç takibi/seyri/kargo takip gibi alanlarda yaygın bir şekilde kullanılmaktadır. Sistem aynı zamanda zaman senkronizasyonu içerdiğinden finans, telekomünikasyon veya bilgisayar ağları kritik zaman güncellemelerinde kullanılmaktadır. Gps uydulardan alınan radyo frekansları ile anlık mevkiyi belirlemeye çalışır. Sistem uydu, kontrol ve kullanıcı segmentlerinden oluşmaktadır. Uzay segmenti uyduları ve radyo frekanslarını, kontrol segmenti kara monitör istasyonlarını, uydu takibini ve senkronizasyon kontrollerini içerirken kullanıcı segmentinde ise bu frekansların Gps alıcıları tarafından yorumlanarak seyir amaçlı kullanılmasına yaramaktadır. Toplamda 24 uydu ve 6 farklı orbit düzlem üzerinde ve dünyadan yaklaşık 20.000 km yükseklikte kesintisiz hizmet verebilmektedir. Frekanslar 1575.42 mhz ve 1222.6 mhz iken dalga boyu 19 cm ve 24 cm'dir. Anlık mevkiyi ise en az 4 uydudan aldığı frekanslarla belirlemekte olup uydu şeması aşağıdaki gibidir (Rasmussen ve Diğerleri, 2011).

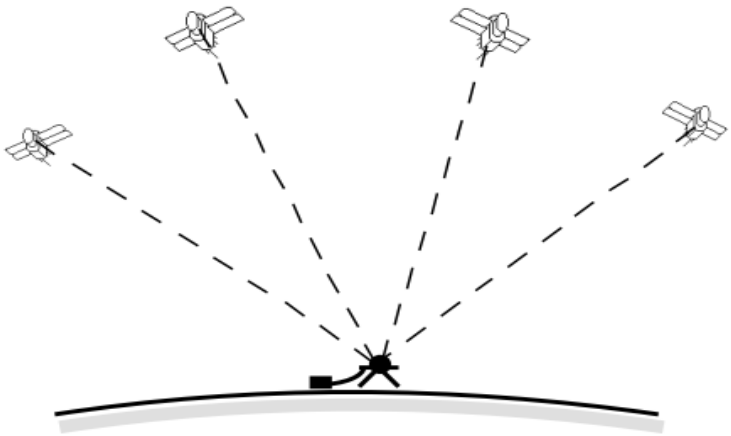
Şekil 8 ve 9'da Gps ve uydu sistemi şematize edilmiş hali gösterilmiştir.

Şekil 8: Gps –Uydu Sistemi



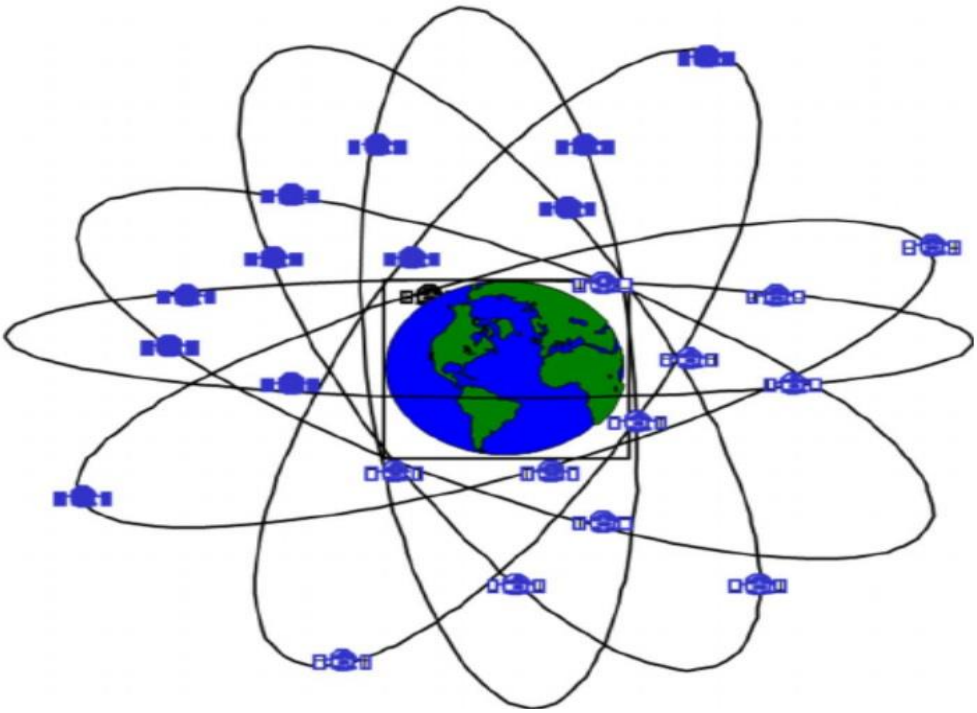
Kaynak: Liu, 1993: 88.

Şekil 9: Gps Ais Sistemi



Kaynak: Liu, 1993: 88.

Şekil 10: GPS Pozisyon



Kaynak: Liu, 1993: 87.

Şekil 9'da Gps –Uydu sistemi ve Şekil 10'da ise Gps pozisyon sistemi gösterilmiştir. Gemiler radyo frekans temeli seyir yaptığından ötürü, frekanslarda oluşturulacak sıkışıklık, bozukluk veya engellemeler geminin güvenliğini ve emniyetini tehlikeye atıp ciddi zararlara sebebiyet verebilmektedir. Jammer (sinyal bozucu) olarak bilinen cihazlarla sinyallere zarar vererek geminin emniyetini tehlikeye atan bu cihazlar piyasada oldukça düşük miktarda ücretlerle satışı yapılmaktadır. Gps üzerinden alınan hatalı bilgiler gemideki entegre sistemlerin hepsinin yanlış bilgi vermesine sebebiyet vermektedir (Miller, 2018: 12).

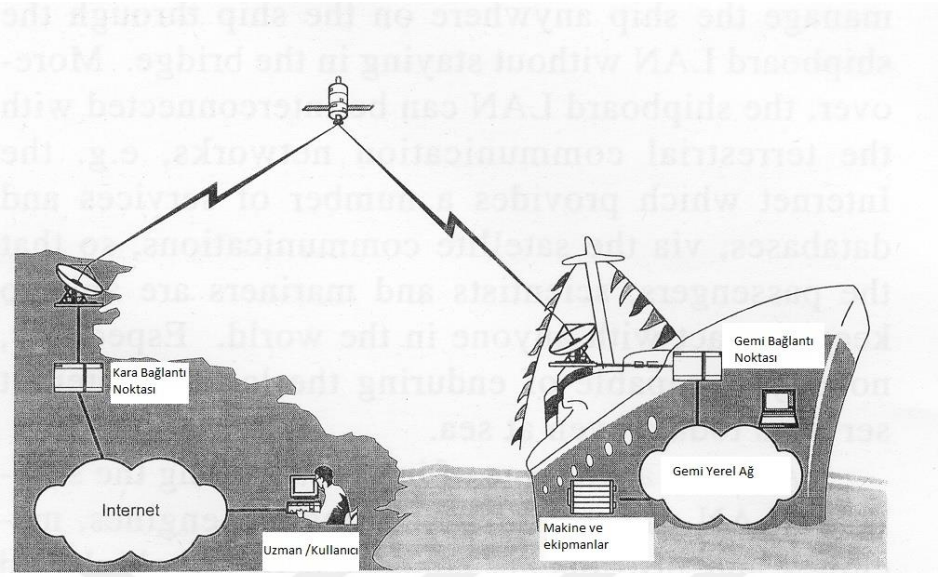
2013 yılında Texas Üniversitesinde yapılan bir araştırmada hackerların ortadaki adam saldırısıyla uydu sinyallerini aldatıp kara istasyonuna yanlış bilgilendirmede bulunmuştur. Sinyaldeki frekans ve güç arttıkça gemi sinyallere güvenmeye başlamakta ve gemiye yanlış bilgiler sağlayarak ofis ve gemiyi yanlış yönlendirerek ciddi tehlike ve zararlara sebebiyet vermektedir. Bu tip durumlarda gemi personelinin durum farkındalığı oldukça önem arz etmektedir (Utnews, 2019).

2.4. Inmarsat ve İletişim Sistemi

Yerel bağlantı ağları (local area network – lan) sayesinde ticari gemilerde otonom sistemlere bağlanmak hem daha pratik hem de zaman kaybını önlemektedir. Gemilerdeki zabitan ekibi köprüüstünde olmaya gerek kalmaksızın geminin herhangi bir yerinden işlemlerini bu ağ sayesinde yapabilmektedir. Bu sistemlere aktarılan uydu veya internet bağlantıları sayesinde gemideki personel veya yolcular da dünyanın her yerine iletişim sağlayabilir konuma gelmektedir.

Önemli olan bir diğer avantaj ise yerel ağlara entegre internet sayesinde gemi makinesi veya kontrol ünitelerine karadan veya teknik servis tarafından uzaktan erişim sağlanarak sorunların çözülebilmesidir. Karmaşık bir bağlantı sisteminin olması arıza durumunda gemi personeli tarafından müdahale edilmemesine sebebiyet vermekle beraber, sistem aktif durumdayken acil durumlarda karadan hızı ve pratik müdahalelere imkân sağlamaktadır. Gemi-kara bağlantı şeması ise Şekil 11'de gösterildiği gibidir.

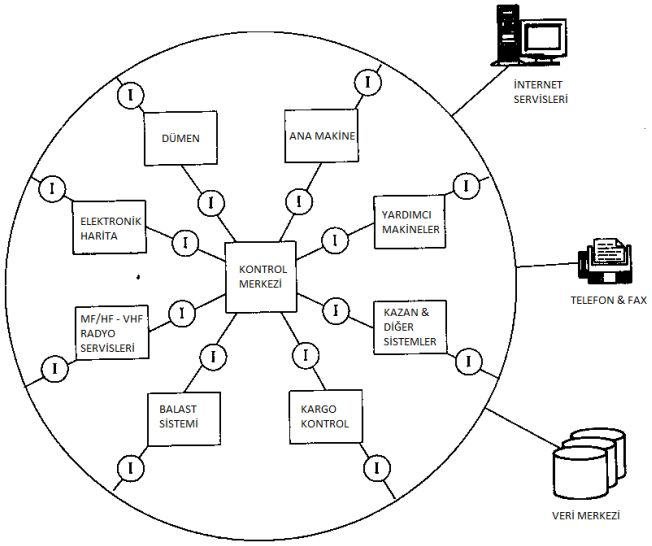
Şekil 11: Gemi-Kara Bağlantı Şeması



Kaynak: Chou ve Juang, 1993: 35

Gemi tabanlı yerel bağlantı sisteminde tüm kontrol noktaları, makine, yardımcı makineler, kargo kontrol, balast sistemleri ve diğer bilgisayarlar tek yerel ağ üzerinden bağlı olup kontrolü daha kolay hale getirmektedir. Sisteme uydu telefonu veya uydu tabanlı internet erişimi de sağlanarak daha pratik hale gelmektedir. Örnek figür ise Şekil 12'deki gibidir.

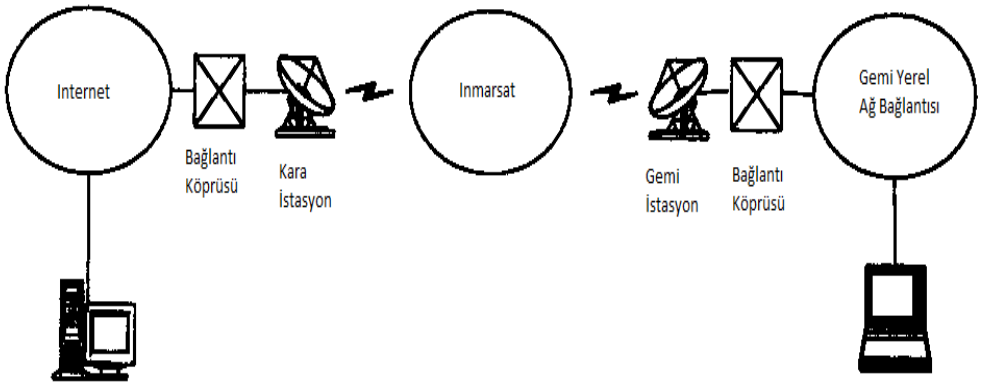
Şekil 12: Gemi Yerel Bağlantı Şeması



Kaynak: Chou ve Juang, 1993: 36.

Inmarsat sistemi 1979 yılından beri tüm denizcilik camiasına global iletişim sağlamaktadır. Gemilerde Inmarsat sisteminin farklı modelleri ile (m, c, f) faks, telefon, veri alışveriş merkezini sağlamaktadır. Inmarsat C ve F sistemleri günümüz gemilerinde en uygun ve en ucuz iletişimi uzunca bir süre sağlamıştır. Gemilerde internet Inmarsat sistemi ve gemilerdeki yerel ağ sistemi arasında yapılacak protokoller sayesinde daha pratik bir şekilde gerçekleştirilmektedir. Yapılan tüm veri alışverişleri NMEA (National Maritime Electronic Association) standartlarına uygun şekilde transfer edilmekte ve veri dönüşümü sağlanmaktadır. Inmarsat internet üzerinden veri alışverişi aşağıdaki Şekil 13'teki gibi sağlanmaktadır. Tüm iletişim süresi boyunca bilgi alışverişi NMEA standartları dâhilinde gerçekleşmektedir.

Şekil 13: Mail İletişim Sistemi



Kaynak: Chou ve Juang, 1993: 46.

Elektronik email ise internet sağlayıcılarda operasyonel manada kullanılan en yoğun hizmetlerden biridir. Inmarsat dışında Vsat veya diğer sistemler üzerinden de internet bağlantıları sağlanmakta olup genel olarak altyapısı Inmarsat sisteminde açıklandığı gibidir. Gemiler arası veya gemi kara bağlantıları kurulurken yapılan saldırılar genelde bağlantı noktalarına (end point) yapılmaktadır. Bağlantı noktaları gemi veya kara istasyonları olabilmektedir. Bu sistemde siber saldırı yapılabilecek 3 ana nokta aşağıdaki gibidir.

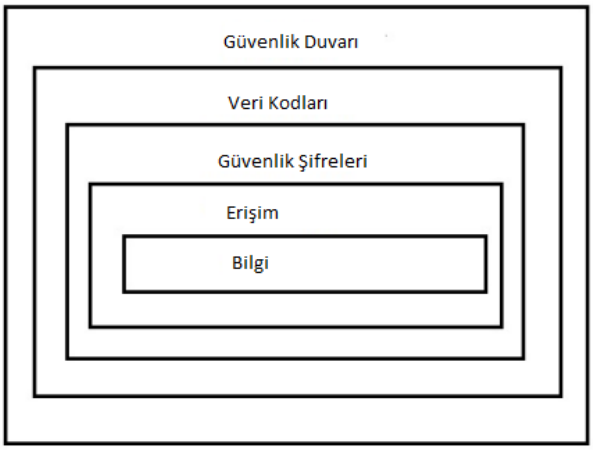
- Gemilerde uydulardan veya Ais ve Vhf sinyal gücü oldukça zayıf olmakla beraber kolayca istasyona yakın güçlü sinyallerle engellenip alt edilebilir durumdadır.
- Gemilerden kara istasyonlarına gönderilen sinyallerde oldukça zayıf güçte olduğundan kolay alt edilip engellenebilir seviyededir.
- İnternet sağlanan gemilerde ise kara istasyonu ve uydular arasındaki sinyallerde manipüle edilebilir seviyede olduğundan saldırıları açık konumdadır.

Gemi ve diğer istasyonlarla yapılan tüm bilgi alışverişleri koruma duvarları (firewall) ve koruma köprüleri (gateway) ile güvenliği sağlanmaya çalışılmaktadır. Karadaki istasyonlardaki karışık yapı, yüksek özel sistemler ve büyük uydular sebebiyle sinyallerde sıkışıklık yaratıp manipüle etmek daha meşakkatlidir. Önceki bölümlerde de bahsettiğimiz siber saldırılar ve insan hataları da hesaba katıldığında sistemdeki güvenlik eksikliği sebebiyle yapılacak olan saldırılar ve oluşacak zararlar düşünüldüğünde durum oldukça önem arz etmektedir (Lee ve Rodseth, 2015).

2.5. Güvenlik Duvarı

Güvenlik konusunda yaşanan zafiyetler sebebiyle birçok ağda verilerin korunması amacıyla çeşitli güvenlik yöntemleri uygulanmaktadır. Yaşanan olayların geneli bilgisayar veya ağdaki bilgilere erişip çeşitli manipülasyonlar yaratmaktır. Veriye ulaşana kadar gereken aşamalar Şekil 14'teki grafikte örnek olarak gösterilmiştir.

Şekil 14: Ağ Güvenlik Duvarları



Kaynak: Nguyen, 2019.

Ağlar bilgiye ulaşmayı kısıtlama amaçlı bir sürü koruma içermektedir. Bunlardan ilki erişim hakkıdır. Bilgiye kimlerin erişebileceğini belirler. Diğer koruma yöntemi ise kullanıcı adı/şifre uygulaması olup kullanılan en yaygın sistemlerden biridir. Kullanıcı bütün erişim hakkına sahiptir. Diğer metot ise veri kodlama yöntemidir. Yönetici tarafından bütün bilgiler kodlanarak şifrelenir ve erişim hakkı kısıtlanır. Güvenlik duvarı sistemi ise sisteme istenmeyen bilgi ve linkleri engelleyerek filtreleme görevi görür.

Güvenlik duvarları donanımsal olacağı gibi yazılımsal temelli de olabilmektedir. Donanımsal güvenlik duvarları iletişim kutusu (network box), yönlendirici (router) ve yazılım içermekte olup sadece yazılımsal temelli olanlara göre daha karmaşık bir yapısı bulunmaktadır. Yazılımsa güvenlik duvarlarında seçilen belli işlemler dışında diğer bütün girişleri filtrelemektedir. Veri transferini belli kurallar çerçevesinde kısıtlamaktadır. Genellikle bu tip güvenlik duvarı içeren sistemlerde kısıtlı ve genel ağ olmak üzere iki erişim ağı bulunmaktadır.

Güvenlik duvarının ana görevlerini özetleyecek olursak (Nguyen, 2016: 6);

-İletişim trafiğini yönetip kontrol altında tutmak,

-Sınırlı erişim sağlamak,

-Kaynakları korumak,

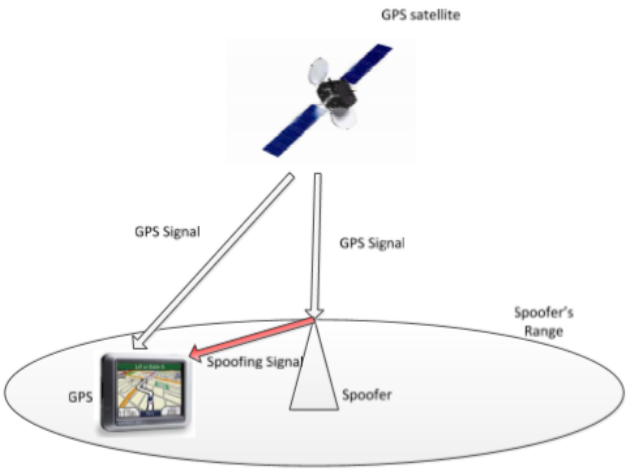
-Olayları kayıt altına alıp raporlamak.

ÜÇÜNCÜ BÖLÜM
GEMİ SİBER ATAK SENARYOLARI

3.1. GPS ALDATMA

Gps sinyalleri tüm ticari cihazlarda düşük frekanslarda kullanılmaktadır. Bu durumda daha güçlü frekanslar yaratabilecek yapılar düzenlenebilir. Bu durum Gps tarafından da tanımlanan sinyaller yerine yanlış sinyallerin algılanmasına sebebiyet vermektedir. Cihazda yer alan time delay (zaman uzaklığı; cihaz konumunun uydu uzaklığını belirlemektedir) düzenin aldatılmasıyla konumlarda hatalı bilgiler oluşmasına sebebiyet vermektedir. Gemideki seyir cihazları konum bilgisini Gps üzerinden alması sebebiyle ciddi kazalara neden olabilmektedir. Örnek Gps sinyal sistemi ise Şekil 15'te gösterilmiştir.

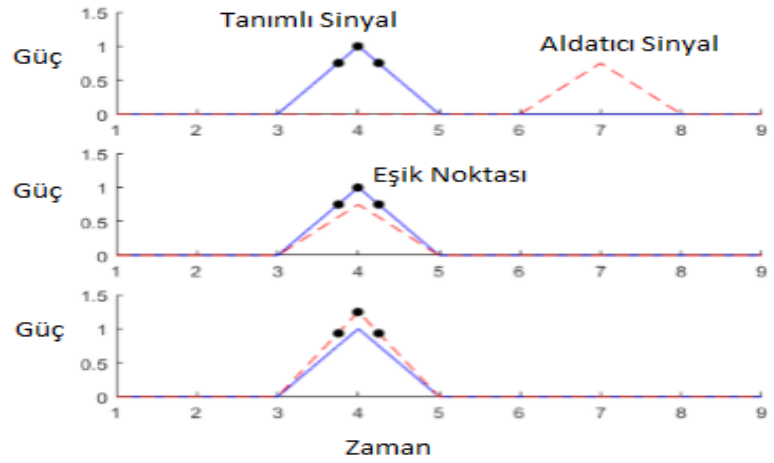
Şekil 15: Gps Sinyal Sistemi



Kaynak: Zhang, 2013: 39.

Tanımlı sinyallerden daha güçlü frekansların yayınlanması ve hedefe yönlendirilmesi sonucunda sinyal sıkışıklığına (jamming) ve saldırgan tarafından kontrolün ele geçmesine sebebiyet verebilmektedir. Bu durum Gps cihazının kilitlenmesine veya yanlış pozisyon bilgileri verip gemiyi aldatmaya sebebiyet verebilmektedir.

Tablo 6: Sinyal Güç Dengesi



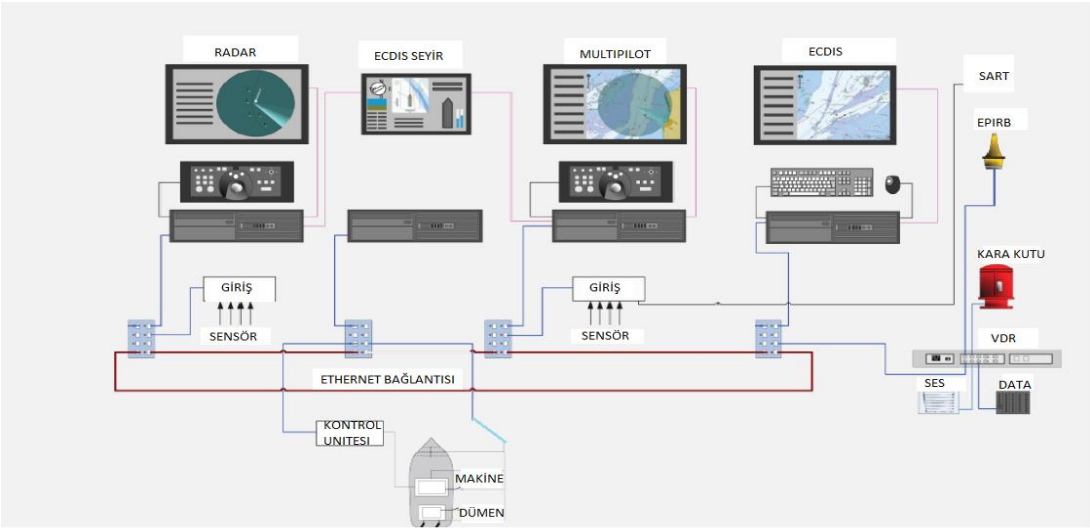
Kaynak: Chapman, 2017.

Tablo 6'da görüldüğü gibi aldatıcı sinyaller ve Gps tanımlı sinyaller arasındaki zaman güç dengesi gösterilmiş olup gerekli aldatıcı sinyal gönderildiğinde Gps aldatması gerçekleşmektedir (Chapman, 2017: 17). Günümüzde ise daha çok drone (uzaktan kumandalı araçlar) üzerine saldırılar yapılıp yanıltma/aldatmalara sebebiyet vermektedir. Dolayısıyla yanıltılan Gps ile yapılacak seyir oldukça tehlike arz etmekte olup ciddi boyutlarda kazalara sebebiyet verebilir.

3.2. VDR YANILTMA

VDR (voyage data recorder) gemilerin kara kutusu olarak bilinen yolcu ve 3000 grosston üzerindeki tüm gemilerde zorunlu hale getirilmiştir. Cihaz herhangi bir kaza sonrasında veri depolayıp gün yüzüne çıkarılmayı sağlamaktadır. Cihazın veri ünitesi geminin tüm bilgilerini depolamaktadır. Depolanan bilgiler ise şu şekildedir; Vhf, Radar, takılan hard disk veya flaş diskler, mikrofonlar, alarmlar, sensörler ve ilgili diğer tüm veriler depolanmaktadır. Veri kayıt biçimi ise; tarih ve saat, gemi pozisyonu, Gyro, Radar, köprüüstü konuşmaları, radyo konuşmaları, derinlik, birincil alarmlar, sensörlü kapıların durumları, dümen ve makine durumlarını güncel olarak kayıt altına almaktadır. Vdr sistemindeki en büyük zaaf ise, sistemin güncellemelerinin usb flaş, harddisk, internet üzerinden yapılıyor ve dışarıdan müdahaleye açık olmasıdır. Genellikle Windows temelli yazılım kullanılması aldatıcı saldırılara daha çok maruz kalmasına sebep olmaktadır. Cihazın tüm sistemle entegre olması durumu daha tehlikeli konuma sokmaktadır. Bu tip saldırılar olduğunda sistemin otomatik geri bildirim sistemi taşıması hayati önem taşımaktadır (Lagouvardou, 2018: 71). Örnek Vdr bağlantı diyagramı ise Şekil 16'da ki gibidir.

Şekil 16: VDR Bağlantı Diyagramı



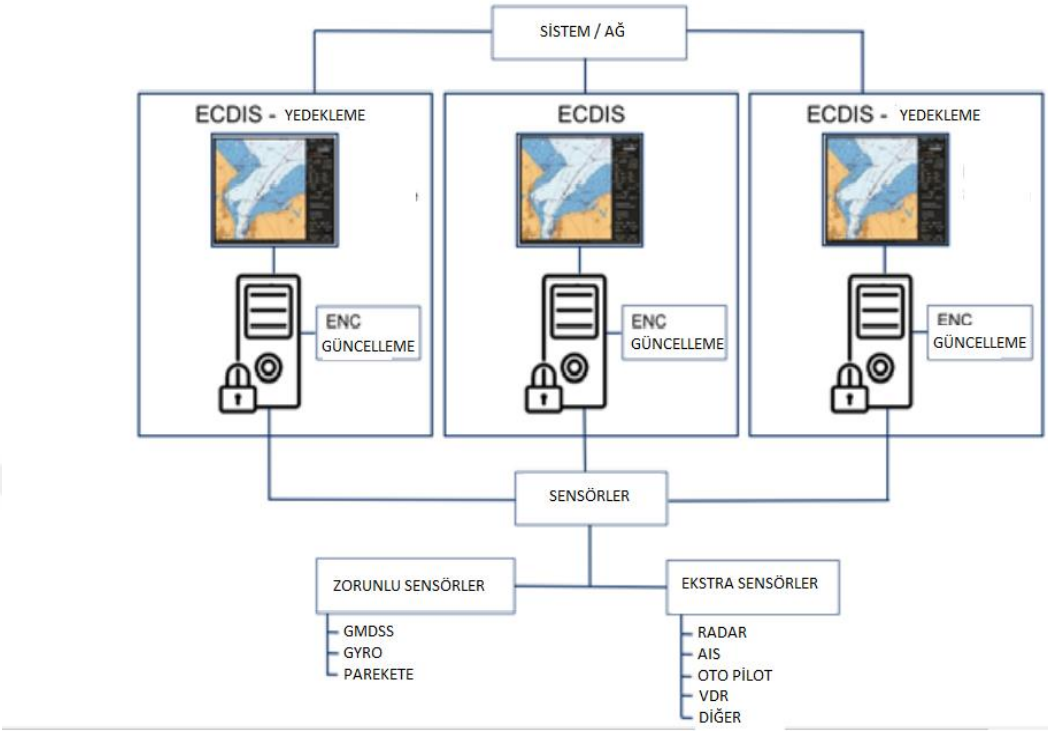
Kaynak: Wartsila, 2019.

VDR sistemi tüm yedeklemelerini genellikle Windows temeli üzerinden yapmış olduğundan sisteme sızan bir virüs veya saldırgan tarafından değiştirilip silinmesine neden olabilir. Bu gibi durumlar herhangi bir olayın açığa çıkmasını veya üstünün sehven kapatılmasına sebebiyet vermektedir. Hindistan'da vuku bulmuş, ticari geminin bir balıkçı gemisine çarpması sonucu oluşan kazada Vdr sistemine müdahale edilerek kayıtlar tekrar düzenlenmiş hukuk dışı bir olaya sebebiyet verilmiştir.

3.3. ECDIS ATAK

Ecdis IMO tarafından zorunlu kılınan ve tüm köprüüstlerin de bulunması gereken bir cihazdır. Ecdis programları güvenlik açısından birçok eksiği bulunmaktadır. Genellikle Ecdis sistemi bilgisayarlardaki programlar üzerinden çalışmakta (Windows XP) ve güncellemesi sürekli yapılamayan bu programlar birçok saldırıya açık hale gelmektedir. Sisteme haritalar dvd, flaş disk veya internet üzerinden yüklenmektedir ve köprüüstündeki diğer cihazlarla entegre bir şekilde çalışmaktadır, bu durum saldırgan için geniş bir ağa ulaşmasına olanak sağlamaktadır. Aldatıcı içeriklerle sistemi ele geçiren saldırgan haritaları silip ve değişikliğe uğratıp geminin kaza yapmasına veya daha ciddi hasarlar vermesine sebebiyet verebilmektedir (Bothur, 2017: 4).

Şekil 17: Ecdis Sistemi



Kaynak: Svilicic ve Diğerleri, 2019: 2.

Ecdis bağlantı şeması ise Şekil 17'deki gibidir. Ecdis kötülümcül yazılımlar (malware) tarafından yapılan saldırılara karşı savunması düşük seviyelerde olup sisteme enfekte edilen virüsler tarafından ciddi zararlar verilebilecek bir sistemdir. Usb flash bellek, CD veya internet üzerinden atılan sahte mail yoluyla kurulan kötülümcül yazılımlar sistemi ele geçirmekte dolayısıyla hatalı eksik haritaların yüklenip tüm cihazları aldatmaktadır.

Dolayısıyla sistem güncellemeleri internet veya mail yolu ila alınıyorsa mutlaka anti virüs veya güvenlik programları kullanılmalı tehlikeli bir şey fark edildiğinde geri bildirim sistemi oluşturulmalıdır. Sistem güncellemeleri usb flaş veya cd üzerinden yapılıyorsa önce dâhili olmayan bilgisayarda taranmalı ardından sistem güncellemesi sağlanmalıdır.

DÖRDÜNCÜ BÖLÜM

TÜRK GEMİ İŞLETMECİLERİ ÜZERİNE İNCELEME

4.1. ARAŞTIRMANIN AMAÇ VE KAPSAMI

Araştırmanın amacı Türk gemi işletmecilerinin siber güvenlik üzerine yaptıkları çalışmaların analizini yapmaktır. Bu amaç doğrultusunda denizcilik firmalarının bilişim departmanı yetkilileriyle görüşme sağlanmıştır. Araştırmamızın temel amacının gerçekleştirilmesi için alt amaçlar da belirlenmiştir. Araştırma sonucunda siber güvenlik konusunda şirketlerin siber güvenlik politikaları incelenmiş ve önerilerde bulunulmuştur.

4.2. ARAŞTIRMANIN YÖNTEMİ VE KISITLAR

Bu çalışmada 1. ve 2. el veriler kullanılmıştır. Uluslararası ve ulusal raporlar, yapılmış olan tezler, makaleler ve internet veri tabanları incelenmiş ilgi detaylar kaynakça bölümünde listelenmiştir. Son bölümde ise veri toplama aracı olarak konu ile alakalı uzmanlarla görüşme yapılmıştır. Yapılan görüşmede kullanılan sorular ekte sunulmuştur. Araştırmanın evrenini Türk gemi işletmecilerinde aktif olarak görev yapan bilişim departmanı yetkilileri oluşturmaktadır. İlgili yetkililerle telefon görülmesinin ardından mail yoluyla ilgili sorular iletilmiş ve yazılı olarak yine mail yoluyla alınarak kayıt altına alınmıştır.

4.3. ARAŞTIRMANIN ÖNEMİ

Denizcilik alanında teknolojinin payı yükseldikçe sektör içerisinde kullanılan elektronik cihaz ve yazılımların önemi ve payı artmaktadır. Bunlara paralel olarak bu teknolojinin güvenliği oldukça önem arz etmektedir. Yapılacak siber saldırılar ile önemli bilgilerin çalınmasına manipülasyonların yaratılmasına veya şirketlere ciddi mali zararların verilmesine neden olur. Bu konuda bu alana gerekli yatırımın ve önemin verilmesiyle beraber çalışanlarda farkındalık seviyesinin yükseltilmesi alınabilecek gerekli önlemlerdir. Bu araştırma Türk gemi işletmecilerin siber güvenlik konusundaki önlemleri ve politikaları analiz edilmiştir.

4.4. BULGULAR VE DEĞERLENDİRME

Araştırmaya 14 denizcilik şirketi bilişim departmanı yetkilisi ve 31 denizcilik firmasına bilişim desteği veren özel bir bilişim kuruluşunun yetkilisi katılmıştır. Bilişim departmanı yetkilileri ile telefon görüşmesine müteakip mail yoluyla aşağıdaki sorular iletilmiş ve yine yazılı olarak mail yoluyla cevaplar alınmıştır. Yetkililerin profil bilgileri ise Tablo 7'deki gibidir.

Tablo 7: Katılımcı Profil Bilgisi

Katılımcı	Diploma Derecesi/Bölüm	Görevi	Tecrübe	Görüşme Yöntemi
K1	Lisans / İşletme	Bilişim Uzmanı	7 yıl	Telefon + Mail
K2	Lisans / Bilgisayar Mühendisi	Bilgi-İşlem Uzmanı	12 yıl	Telefon + Mail
K3	Lisans / Elektrik Mühendisi	Bilişim Uzmanı	9 yıl	Telefon + Mail
K4	Lisans / Bilgisayar Mühendisi	Yazılım Geliştirme Müdürü	12 yıl	Telefon + Mail
K5	Lisans / Gemi İnşa Mühendisi	Bilişim Departmanı Müdürü	20 yıl	Telefon + Mail
K6	Ön lisans / Bilgisayar	Teknik Asistan	3 yıl	Telefon + Mail
K7	Ön lisans / İletişim	Teknik Destek	4 yıl	Telefon + Mail
K8	Lisans / Turizm	Satın Alma Uzmanı	10 yıl	Telefon + Mail
K9	Lisans / Bilgisayar Mühendisliği	Bilgi Teknolojileri Uzmanı	6 yıl	Telefon + Mail
K10	Ön lisans / Yazılım	Teknik Destek	5 yıl	Telefon + Mail
K11	Lisans / Matematik	Teknik Müdür	20 yıl	Telefon + Mail
K12	Lisans / İletişim	İletişim Uzmanı	12 yıl	Telefon + Mail
K13	Lisans / Makine Mühendisi	Enspektör	6 yıl	Telefon
K14	Lisans / İşletme	Operasyon Müdürü	7 Yıl	Telefon
K15	Lisans / Ticaret	Operasyon Müdürü	5 yıl	Telefon

Katılımcılar en az 3 yıl en fazla ise 20 yıl tecrübelidir. Ortalama tecrübe ise 9,2 yıldır. 3 katılımcı ön lisans mezunu iken 12 katılımcı da lisans mezunudur. Katılımcıların 12 tanesine telefon ve mail yoluyla ulaşılırken 3 tanesine telefon yoluyla ulaşılmıştır.

Yetkililere yönelttiğimiz ***' Şirketinizin siber güvenlik politikası var mı? '*** sorusuna 11 şirketin siber güvenlik politikasının olduğunu, kendi bilişim departmanı olmasına rağmen 3 şirketin siber güvenlik politikası olmadığını aynı zamanda bilişim

desteği alan 31 şirketin siber güvenlik politikasının olmadığı sonucu ortaya çıkmaktadır.

Yetkililere yönelttiğimiz ***'Şirket ve gemilerde siber saldırı karşın nasıl önlemler alınmaktadır? Kullanılan koruma programları hangileridir?'*** soruna aldığımız cevap Tablo 8'de belirtilmiştir.

Tablo 8: Kullanılan Güvenlik Uygulamaları

Katılımcı	Güvenlik Duvarı	Antivirüs	Uç uca şifreleme	Donanımsal ekstra güvenlik
K1	✓	✓	✓	✓
K2	✓	✓	✓	✓
K3	✓	✓	✓	✓
K4	✓	✓	✓	✓
K5	✓	✓	-	✓
K6	✓	✓	-	✓
K7	✓	✓	-	✓
K8	✓	✓	-	✓
K9	✓	✓	-	✓
K10	✓	✓	-	✓
K11	✓	✓	-	✓
K12	✓	-	-	-
K13	✓	-	-	-
K14	✓	-	-	-
K15	✓	-	-	-

Şirketlerin tamamı güvenlik duvarı uygulaması kullanıyorken bu siber saldırı için yeterli önlem olarak görülmemektedir. Siber politikanın mevcut olduğu firmalarda ise bu durum uç uca şifreleme, anti virüs ve donanımsal ekstra güvenlik uygulamalarıyla desteklenerek güvenlik seviyesi artırılmaya çalışılmaktadır. Tablo 8'de ki 15 numaralı katılımcı 31 firmaya bilişim desteği veren kuruluşun yetkilisi olarak yer almakta olup bu şirketlerde ekstra hiçbir güvenliğin alınmadığı görülmektedir.

Bu durum siber politikasının olmamasına paralel seyretmektedir. Bu soruya bilişim desteği veren firmanın temsilcisi ise şu şekilde cevap vermiştir,

''Virüs programı olarak Trend Micro kullanıyoruz gemilerde internet sürekli bir problem olduğu için tam anlamıyla bir virüs programı çalışamıyor çalışsa bile updateler de geri kalıyor.''

İnternet erişimi sağlanamayan gemilerde güncellemelerin yapılamaması, siber saldırılara karşı güvenliği düşük seviyelere çekmektedir. Yapılan yazın taramasında tam anlamıyla internet erişimi sağlanan gemilerde de ulaşım kolaylığı açısından saldırıya uğrama riski de paralel olarak artmaktadır.

Yöneltilen 3.soru ise, ***'Ekibin bu konudaki farkındalığı hangi seviyede ve artırmak amaçlı eğitimler düzenleniyor mu?'*** şeklinde olup alınan cevaplar Tablo 9'da listelenmiştir.

Tablo 9: Uygulanan Eğitimler

Katılımcı	Siber güvenlik Eğitimleri	Uygulamalı Farkındalık Testleri	Eğitim veya test uygulanmıyor
K1	✓	✓	-
K2	✓	✓	-
K3	✓	-	-
K4	✓	-	-
K5	✓	-	-
K6	✓	-	-
K7	✓	-	-
K8	✓	-	-
K9	✓	-	-
K10	✓	-	-
K11	✓	-	-
K12	✓	-	-
K13	✓	-	-
K14	-	-	✓
K15	-	-	✓

Tablo 9'da görüldüğü gibi farkındalık testlerini yalnızca iki şirket uygulamakta olup bu durum oluşabilecek herhangi bir saldırı durumunda uygulanmayan diğer şirketlerde birçok eksikliğe sebebiyet verebilecektir. Uygulamalı testler ile personelin siber olaylara aşinalığı, anlık olarak yapılması gerekenleri daha iyi öğrenmesi ve güvenlik bilincinin oluşturulmasına katkı sağlamaktadır.

Güvenlik eğitimleri mail yoluyla/haber bültenleri paylaşımıyla/şirket içi sunum veya eğitimlerle gerçekleştirilmektedir. Bu soruya aldığımız cevaplardan biri de şu şekildedir,

> *''Eğitim kanayan bir yara ne kimsenin vakti ne de kimsenin buna ayıracak bütçesi var''*

Şirketlerin bu konuya zaman ve maddiyat ayırması oldukça önemli olmasına rağmen bu konuda bazı şirketlerin bütçe dahi ayırmadığın görmekteyiz. Bilişim desteği veren şirket yetkilisinin cevabı ise şu şekilde olmuştur,

> *''Siber saldırılar için ben şu ana kadar hiç bir firmada eğitim görmedim biz müşterilere Firewall satarken bile büyük problem yaşıyoruz ve önemi yok ki bilgisi bile geliyor''*

Önceki cevaba paralel olarak siber güvenlik konusunda yetersiz kalmanın en büyük sebeplerinden biri de şirketlerin bu duruma ayırdığı bütçe olaraktan değerlendirebiliriz. Siber güvenlikte yetersiz kalma konusunda aldığımız en detaylı cevaplardan biri de şu şekildedir,

> *''Tüm altyapı ve bileşenleri siber saldırılara karşı birçok noktada güvenlik önlemleri ve çözümleri ile korunmaktadır. Taşınabilir tüm cihazlarda DLP ve Çok katmanlı koruma yazılımları çalışmaktadır. Gemiler ve kurum ile iletişim tüm noktalardan VPN üzerinden sağlanmakta, erişimlerin tamamı, SIEM araçları ile olası saldırı veya tehditlere karşı izlenmektedir. Ürün ismi vermemiz ne yazık ki güvenlik politikalarımız gereği mümkün değil. Fakat piyasadaki en kabul görmüş ürünlerin kullanıldığını söyleyebilirim.''*

Konu hakkında alınan en detaylı önlemlerden olup yalnızca bir firmada görebildiğimiz siber güvenlik eğitim ve uygulamalarıdır. Bu durumun sadece bir şirketle kalmamalı ve tüm şirketlerde olmalıdır.

Yetkililere yönelttiğimiz 4.soru ise, ***'Sektörde gelişen saldırı ve oluşan maliyetler düşünüldüğünde, böyle bir duruma maruz kalınırsa nasıl bir yol izlemeyi planlıyorsunuz?'*** Şeklinde olup cevaplar Tablo 10'da sıralanmıştır.

Tablo 10: Eylem Planları

Katılımcı	Siber Olaylara Müdahale Ekibi	Felaket ve Kriz Yönetimi Uygulamaları	Yedekleme Prosedürleri	KVKK Bildirimi ve Uygulamaları	Herhangi Bir Eylem Planı Yok
K1	✓	-	-	-	-
K2	-	✓	-	-	-
K3	-	-	✓	-	-
K4	-	-	✓	-	-
K5	-	-	✓	-	-
K6	-	-	✓	-	-
K7	-	-	-	-	✓
K8	-	-	-	✓	-
K9	-	-	-	-	✓
K10	-	-	-	-	✓
K11	-	-	-	-	✓
K12	-	-	-	-	✓
K13	-	-	-	-	✓
K14	-	-	-	-	✓
K15	-	-	-	-	✓

Tablo 10'da görüldüğü gibi oluşabilecek herhangi bir siber saldırıya karşın şirketlerin büyük çoğunluğunun eylem planı bulunmamaktadır. Bu durum oluşabilecek eylem sonrası maddi hasarın büyümesine ve tekrar toparlanmanın ciddi zaman kaybına sebebiyet vereceğini göstermektedir.

Bu durum firma imajına da ciddi zarar vermektedir. Bu soruya aldığımız cevaplardan biri de şu şekildedir,

> *''Hangi sektör olursa olsun risk almayı seviyoruz bize bir şey olmaz olsa da bir şekilde hallederiz mantığı şu an hâkim, tabi biz bu durumun ortaya çıkmaması için elimizden geleni yapıyoruz. Eğer böyle bir durum ile karşılaşırsak kullandığımız her programın saat bazında yedekleri mevcut onlardan geriye döneceğiz umarım hiç olmaz. ''*

Önceki sorulara aldığımız cevaplara paralel olaraktan şirketlerin bu konuya zaman ve bütçe ayırması paralelinde siber güvenlik seviyesinin daha yukarı çıkmasını sağlayacaktır.

Yetkililere son sorumuz ise şu şekilde olmuştur, ***''Sirketinizin siber güvenlik seviyelerinin artırılması hususunda görüş ve önerileriniz nelerdir?''*** Bu soruya aldığımız cevap ise Tablo 11'de görülmektedir.

Tablo 11: Öneriler

Katılımcılar	Farkındalık Eğitimlerinin Artırılması	İhtiyaç duyulmamaktadır	Düzenli Güncellemeler	Penetrasyon Testlerinin Artırılması
K1	✓	-	-	-
K2	✓	-	✓	-
K3	✓	-	-	-
K4	✓	-	-	✓
K5	✓	-	-	-
K6	-	-	✓	-
K7	-	-	✓	-
K8	-	✓	-	-
K9	-	✓	-	-
K10	-	✓	-	-
K11	-	✓	-	-
K12	-	✓	-	-
K13	-	✓	-	-
K14	-	✓	-	-
K15	-	✓	-	-

Bu konuda herhangi bir eğitim ve uygulama yapmayıp ihtiyaç duyulmamaktadır cevabı veren şirket yetkililerinin sayısı oldukça yüksektir. Bu durum siber güvenlik ile alakalı yeterli bir bilgiye sahip olunamadığının dolayısıyla gemi veya şirket personelinde güvenlik bilincinin oluşturulmasının bu şartlarda zor olduğu gözükmektedir.

Bu soruya verilen detaylı cevaplardan biri de aşağıdaki gibi olup siber güvenliğin önemi kavrandıkça diğer şirketlerde uygulanması gereken adımlardandır,

> *''Siber güvenlik bakış açısında en zayıf halka olarak "insan" görülmektedir. Bu sebeple siber güvenlik farkındalık eğitimleri bu konuda yüksek önem kazanmaktadır. Sadece güvenlik uzmanlarının değil tüm kurum çalışanlarının bu bilinçte olması ve bu konuda kendisini geliştirmeye hevesli olması gerekmektedir. Güvenlik konusu çoğu zaman sıkıcı olarak görüldüğünden, oyunlaştırma ile daha etkili ve verimli bir eğitim planlanabilir.''*

Uygulama konusunda oyunlaştırma ve uygulamalı testler güvenlik bilincini daha üst seviyelere taşıyacaktır.

SONUÇ

Yapılan görüşmeler sonucunda kurumsal yapıya ulaşmış şirketlerde bilişim (IT) departmanı olduğunu ve dolayısıyla bir siber politikasının mevcut olduğunu görmekteyiz. Bu politikanın sürekli güncel tutulması ve globalleşen dünyada sürekli güncellemelerin yapılması oldukça önemlidir. Güvenlik duvarları, uç uca şifreleme (end of cyrption), anti virüs programları veya donanımsal güvenlik cihazları kullanılmaktadır. Tam anlamıyla internet erişimi sağlanabilen gemilerde dışarıdan gelebilecek saldırılarda açık hale gelirken, internet erişimi kısıtlı gemilerde ise güncellemeler zamanında yapılamadığı için yine yapılabilecek saldırılara açık hedef haline gelmektedir.

Donanımsal güvenlik konusunda uygulanan örnek uygulamalardan biri de dışarıdan usb disk erişiminin kısıtlanmasıdır. Kurumsal firmalarda bu tip uygulamalar yapılıyor iken diğer firmalarda (dışarıdan bilişim desteği alan) bu durum gözlenmemektedir. Bulut güvenlik uygulaması, çok katmanlı yazılımlar, Ethernet kablo kilitleri kullanılan diğer güvenlik uygulamalarıdır.

Genel olarak kurumsal firmalarda siber politika mevcut iken dışarıdan bilişim desteği alan firmalarda böyle bir politika yer almamaktadır. Bu durum firmaları oluşabilecek saldırılara karşı açık hedef haline sokmaktadır. Kullanılan programlar açısından en yaygını güvenlik duvarları olduğunu görmekteyiz. Kurumsal firmalarda bu programa ekstra olarak kullanılan uygulamalarda bulunurken diğer firmalarda bu durum gözlenmemektedir. Kullanılan programların çeşitliliği ve sürekli güncel tutulması oluşabilecek saldırılara karşı alınabilecek en önemli emniyet adımlarıdır.

Şirket ve gemi personelinin bu konudaki farkındalığı en önemli noktadır. Şirketlerde yapılan eğitimler ve rutin bazda gemilere mail yoluyla yapılan bilgilendirmeler bulunmaktadır. Dışardan destek alan şirketlerde ise bu durumda maalesef mevcut değildir.

Her ne kadar sürekli güncelleme ve bilgilendirmeler yapılsa da gemi personelinin henüz okul döneminde bu eğitim ve farkındalığını oluşturulması oldukça önem arz etmektedir. Tezimizin 1.bölümünde Maersk siber saldırılarından bahsetmiştik. Her ne kadar güvenlik önlemleri üst seviyede de olsa en zayıf halka insandır ve insana yapılacak farkındalık eğitimi yatırımları oldukça önem arz etmektedir. Farkındalık bilincinin oluşturulması alınabilecek en emniyetli

önlemlerden olacaktır. Bu konudaki aldığımız görüşlerden biri de eğitim bütçesinin şirketlerde yeterli seviyede olmadığıdır.

Oluşabilecek saldırı ve sistem alt edildiğinde izlenecek yollar ise şu şekilde olduğu görülmektedir. Kurumsal firmalarda siber olaylara müdahale ekibi, kriz ve felaket yönetimi uygulamaları, yedekleme prosedürleri, kvk kurum bildirim ve prosedürleri, acil durum eylem planları bulunmaktadır. Bu noktada en önemli eksiklerden biri de bu durumun uygulamalı olarak senaryolaştırılması ve herhangi bir olayda verimli ve hızlı cevap verebilme durumudur. Dışarda bilişim desteği alan firmalarda bu tip eylem planları olmamakla beraber şirket ve gemi personel eğitim/farkındalığı bulunmamaktadır. Bu konuya şirketlerin zaman ve maddiyat ayırması da oldukça önem arz etmektedir.

Güvenliğin artırılması hususunda ise en zayıf halka olarak görülen insan üzerine eğitim ve bütçenin artırılması, bağımsız ağ kullanımları, güncellemeler, ileri teknoloji kullanımı ve penetrasyon testlerinin artırılması şirketlerin güvenliğin üst seviyelere taşımasını sağlayacaktır. Sonuç olarak insan temelli eğitim ile farkındalığın artırılması aynı zamanda güvenliğe ayrılan bütçe ve zamanın artırılması şirketlerde güvenliği daha üst seviyelere taşıyacaktır.

Araştırmanın Kısıtları

Araştırmanın uygulama kısmında birtakım kısıtlar ile karşılaşılmıştır. İlk olarak bir kısım şirketlerin siber güvenlik politikaları hakkında yine siber güvenlik politikası gereği bilgi paylaşımında bulunmak istememiştir.

Buna ek olarak şirket yetkililerine yönelttiğimiz birtakım soruları kısmen cevaplayıp bir kısmını ise yine siber güvenlik politikaları gereği cevaplamak istememişlerdir. Kendi bilişim departmanı olan kurumsal firmalara mail veya telefon yoluyla daha rahat ulaşım sağlayabiliyorken, bilişim departmanın olmadığı firmalarda ise bu durum tam tersi vaziyettedir. Şirketlerdeki iş yoğunluk durumuna göre mail atılmış ve ardından telefon yoluyla görüşülmesine rağmen bazı firmalardan dönüş almak zorluğu yaşanmıştır.

Yapılabilecek çalışmalar ve acil durum eylem planları önerileri bilişim yetkilileri tarafından farklı önerilerde bulunulmuş ve bu durum yetkilinin yeterliliği, eğitim seviyesi ve tecrübesine bağlı olaraktan farklılık göstermekte ve bir kısıt oluşturmaktadır.

Gelecek Çalışmalar İçin Öneriler

Araştırmanın kısıtları da dikkate alınarak gelecekte yapılabilecek öneri çalışmalar ise;

* Şirket veya gemi personeli üzerine siber farkındalık üzerine çalışmalar yapılabilir,
* Şirket veya gemilere kötülümcül yazılım veya aldatıcı linkler yollayarak hem program ve donanımların güvenirliği hem de personel farkındalığı ölçmek üzerine çalışılabilir,
* Analiz tüm dünyadaki işletmeciler üzerine ülke veya yük gemi tipi kısıtı belirleyerek yapılabilir,
* Ülkelerin, denizcilik kurumlarının veya şirketlerin siber politikalarının karşılaştırılmalı analizleri yapılabilir,
* Siber güvenlik hususunda gemi kaptanlarının görüşü alınarak ta çalışma genişletilebilir,
* Ülkelerin denizcilik eğitimindeki siber eğitiminin yeri hususunda uluslararası denizcilik örgütünün önerileri kapsamında karşılaştırmalı analizleri yapılabilir.

Çalışmaların uygulama bölümünde danışılan katılımcıların profil, eğitim, yaş ve tecrübeleri doğru analizler yapabilmek açısından önem arz etmektedir.

KAYNAKÇA

Abdul-Mumin S. (2011). *Detectıon of Man In The Middle Attack In Ieee 802.11 Networks.* Kwame Nkrumah University Of Science And Technology: 38.

Abdullah R. Abdollah M. Masud Z. Sahib S. (9 Aralık 2011). https://www.researchgate.net/publication/265033832_Recognizing_P2P_Botnets_Characteristic_Through_TCP_Distinctive_Behaviour, (23.02.2019).

Admiralty. (24 Haziran 2013). *Meeting The Latest Data Protection Standard Ford Digital Charts.* http://blog.admiralty.co.uk/2013/06/24/meeting-the-latest-data-protection-standard-for-digital-charts-2/, (01.03.2019).

Akyıldız M. (2013). *Siber Güvenlik Sızma Test Uygulamları*. Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü. Yayımlanmamış Yükseklisans Tezi: 36.

Balduzzi M. ve Wilhoit K. (2014). *A Security Evaluation of AIS*: 4.

Başar Y. (2015). *Siber Suç Soruşturmalarında Adli Bilişim İncelemeleri*. Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü. Yayımlanmamış Yükseklisans Tezi: 34.

Bell S. (21 Ekim 2013). *Cyber Attacks And Underground Activities In Port Of Antwerp.* https://www.bullguard.com/blog/2013/10/cyber-attacks-and-underground-activities-in-port-of-antwerp.html, (01.02.2019).

Bozgeyik A. (2018). *Gaziantep'te Faaliyet Gösteren Orta Ve Büyük Ölçekli İşletmelerin Siber Güvenlik Yönetim Yaklaşımlarının Analizi*. Hasan Kalyoncu Üniversitesi Sosyal Bilimler Enstitüsü Doktora Tezi: 54.

Bothur D. Zheng G. ve Valli C. (2017). *A critical analysis of security vulnerabilities and countermeasures in a smart ship system*. Edith Cowan University: 4.

Canbek G.ve Sağıroğlu Ş. (2006). *Bilgi Güvenliği ve Bilgi Güvenliği Yönetimi*.

Chapman A. (2017). *Gps Spoofing*. https://sites.tufts.edu/eeseniordesignhandbook /files/2017/05/Red_Chapman.pdf, (30.03.2019): 17.

Chou L. ve Juang J. (1993). *Network Integrated Ship Automatic Systems And Internet Working To The Internet*: 35-46.

Conteh N. ve Schmick P. (2016). *Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks*: 31.

Chou L. ve Juang C. (1993). *Information Security and Piracy*: 35-36.

Db Cyber Tech. (2019). *Marriot Breach White Paper*. https://www.dbcybertech.com/pdf/Marriot-Breach-White-Paper.pdf, (18.01.2019).

Değirmenci Y. (2002). *Ulusal Siber Güvenlik Stratejisi*: 63.

Demirer Ö. (19 Aralık 2009). *Bilgisayar Virüsleri Tarihi*. https://e-bergi.com/y/pc-virus-tarihi/, (07.02.2019).

Dergipark. (2019). http://dergipark.gov.tr/download/article-file/465726, (21.02.19).

Dülger M. (2004). *Bilişim Suçları*: 212.

Gürsoy E. (2015). *Bilişim Yoluyla Dolandırıcılık Ve Korunma Yöntemleri*. Afyon Kocatepe Üniversitesi. Yayımlanmamış Yüksek Lisans Tezi: 81-99.

Inverstormaersk. (2019). *Cyber Attack Update*. http://investor.maersk. com/news-releases/news-release-details/cyber-attack-update, (02.01.2019).

ITU. 2008. *Overview of Cybersecurity*. www.itu.int ›rec›dologin_pub›id=t-rec-x.1205 -200804-i!!pdf-e. (19.07.2019).

Jrc. (2004). *Ais Systems*. http://www.jrc.co.jp/eng/product/discontinued/ jhs182/ system.html. (20.10.2019).

Kaspersky. (2019). Threats: Spyware. https://www.kaspersky.com/resource-center/ threats/spyware, (10.02.19).

Liu C. (1993). *Precise GPS Positioning in the Marine Environment*. University of Caglari: 87-88.

Lee K.ve Rodseth O. (2015). *Secure Communication for E-Navigation and Remote Control of Unmanned Ships.*

Lagouvardou S. (2018). *Maritime Cybersecurity: Concepts, Problems and Models*. Technical University of Denmark: 45-90.

Marpaung J.ve Lee H. (2013). *Dark Seoul Cyber Attack*: 3.

Merriamwebster. (2019). *Cyberseccurity*. http://www.merriam webster.com /dictionary/cybersecurity, (17.01.2019).

Middleton B. (2012). *A History of Cyber Security Attacks*: 21.

Holloway M. *Stuxnet Worm Attack On Iranian Nuclear Facilities*, http://large.stanford.edu/courses/2015/ph241/holloway1/, (18.01.2019).

Maan P. and Sharma M. (2012). *Social Engineering: A Partial Technical Attack*: 557.

Marinetraffic. (2019). *Ships Details: Bomar Radiant*. https://www.marinetraffic.com /en/ais/details/ships/shipid:757422/mmsi:636016943/vessel:BOMAR%20RADIANT , (01.03.2019).

MaritimeDenmark. (22 Eylül 2014). *The Dma Attacked By Hackers*. http://maritimedenmark.dk/?Id=17968, (22.01.2019).

Maritimeexecutive. (10 Ekim 2012). *Irans Offshore Platforms Become Target Of Cyber Attacks.* http://maritimeexecutive.com/article/iran-s-offshore-platforms-become-target-of-recent-cyber-attacks, (22.01.2019).

Nautico. (2019). *Maritime Information Systems: Ecdis*. http://pdf.nauticexpo.com /pdf/maritime-information-systems/ecdis-900/31325-42061 -_9.html, (25.02.2019).

Nccgroup. (2014). *Maritime Cyber Security Threat & Oppourtunities*. https://www.nccgroup.trust/uk/our-research/maritime-cyber-security-threats-and-opportunities/. (01.06.2019).

Ncsi. (2019). National Cybersecurity Index. https://ncsi.ega.ee/ncsi-index, (17.01.19).

Nguyen B. (2016). *Network Security and Firewall ClearOS – A Linux Open Source Firewall*. Helsinki Metropolia University of Applied Sciences: 6.

Outpost24. (3 Aralık 2018). *Top 10 Of The World Biggest Cyberattacks.* https://outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks, Erişim Tarihi: 19.01.2019.

Pajunen N. (2017). *Overview Of Maritime Cybersecurity*. South Eastern Finland University: 21.

Redcom. (2019). *Shipboard Communication.* http://www.redcom.com/markets/shipboard-communications, (23.02.19).

Reuters. (2019). *Us and Iran Sanctions And Shipping.* http://www.reuters.com/article/us-iran-sanctions-shippingidUSBRE89L10X2012102 2 , (20.01.2019).

Rasmussen K. Popper C. Tippenhauer N. ve Capkun S.(2011). *On the Requirements for Successful GPS Spoofing Attacks*.

Şakar C., Köseoğlu. B., Büber M. ve Töz A. (2019). *Are The Ships Fully Secured Against The Cyber-Attacks?.* Dokuz Eylul University Maritime Faculty: 6.

Schmidt A. (Ocak 2013). *The Estonian Cyberattacks.* https://www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks, (18.01.2019).

Securelist. (2018). *Kaspersky Security Bulletin 2018.* https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145/, (12.02.2019).

Silgado D. (2018). *Cyber-attacks: A Digital Threat Reality Affecting The Maritime Industry*. World Maritime University: 44.

Svilicic B. Brcic D. Ve Kalebic D. (2019). *Raising Awareness on Cyber Security of ECDIS: 2.*

Solidthink. (2019). *Watering Hole Cyber Attack*. http://solidthink.com/watering-hole-cyberattack/22415/, (20.02.2019).

Sophoslabs. (2019). *ThreatReport.* https://www.sophos.com/enus/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf. (02.07.2019).

Symantec. (2019). *Threat Report*. https://www.symantec.com/security-center/threat-report, (10.02.2019).

Theguardian. (3 Ekim 2017). *Yahoo Says All Of Its 3bn Accounts Were Affected By 2013 Hacking.* https://www.theguardian.com/technology/2017/oct/03/yahoo-says-all-of-its-3bn-accounts-were-affected-by-2013-hacking, (20.01.2019).

Miller T. (2018). *RiskFocusCyber*. https://maritimecyprus.files.wordpress.com/2018/11/risk_focus-cyber.pdf,12.

Tradewinds. (2018). *Maritime Braces For The Next Cyber Breach.* https://www.tradewindsnews.com/safety/maritime-braces-for-the-next-cyber-breach/2-1-437319, (18.07.19).

Turhan M. (2006). *Siber Güvenliğin Sağlanması, Dünya Uygulamaları Ve Ülkemiz İçin Çözüm Önerileri. Bilgi Teknolojileri ve İletişim Kurumu*. Ankara: 57-58.

UDHB. *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı*. https://www.uab.gov.tr/siber-guvenlik, (18.01.2019).

Unibonn. (2019). *Protective Botnet Counter Measure.* http://four.cs.unibonn.de/fileadmin /user_upload/leder/proactivebotnetcountermeasures.pdf, (23.02.2019).

Usnorton. (2019). *Internet Security: Malware and Ransomware*. https://us.norton.com /internetsecurity-malware-ransomware-5-dos-and-donts.html, (10.02.2019).

Utnews. (29 Haziran 2013). *UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea.* https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/, (02.03.2019).

Wartsila. (2019). *Voyage Data Recorder*. https://www.wartsila.com/marine/build/navigation-and-communication/navigation/voyage-data-recorder-vdr-4360, (01.04.19).

Yaşar H. ve Çakır H. (2015). *Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemler*: 8.

Zhang K. (2013). *Security of GNSS positioning and timing*: 39.

EKLER

15/10/2019

Sayın İlgili,

Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, Denizcilikte Güvenlik Emniyet Çevre Yönetimi Yüksek Lisans Programı kapsamında **Dr. Öğr. Üyesi Kpt. Burak KÖSEOĞLU d**anışmanlığında **"Denizcilikte Siber Güvenlik ; Türk armatörleri üzerine bir inceleme"** başlıklı yüksek lisans tezi için bir uzman görüşü çalışması planlanmıştır.

Siz değerli uzmanımızın görüşlerine ihtiyaç duyduğumuz bu çalışma ile siber güvenlik üzerine inceleme yapilarak durumun belirlenmesi amaçlanmaktadır.

Sorulara vereceğiniz cevaplar hiçbir şekilde bu çalışma dışında kullanılmayacaktır. Denizcilik bilimine yararlı olmasını amaçladığımız bu araştırmaya sağlayacağınız katkılar ve tüm destekleriniz için şimdiden teşekkür ederiz.

İsim Soyisim

Onur Topal

İletişim Bilgileri

+905345769362

Sorular

1. **Şirketinizin siber güvenlik politikası var mı?**
2. **Şirketiniz ve gemilerinizde siber saldırılara karşı nasıl önlemler alınmaktadır? Kullanılan koruma programları hangileridir?**
3. **Ekibinizin bu konudaki farkındalığı hangi seviyede ve artırmak amaçlı hangi eğitimler düzenleniyor?**
4. **Sektörde gelişen saldırı ve oluşan maliyetler düşünüldüğünde, böyle bir duruma maruz kalınırsa nasıl bir yol izlemeyi planlıyorsunuz?**
5. **Şirketinizin siber güvenlik seviyelerinin artırılması hususunda görüş ve önerileriniz nelerdir?**