T.C.
İSTANBUL GEDİK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

TÜRKİYE'DE FAALİYET GÖSTEREN DENİZ TAŞIMACILIĞI İŞLETMELERİNE YÖNELİK SİBER RİSK ANALİZİ İÇİN MATEMATİKSEL MODEL ÖNERİSİ

DOKTORA TEZİ

Saim Atalay KELEŞTEMUR

Uluslararası Ticaret Anabilim Dalı

Uluslararası Ticaret Doktora Programı

AĞUSTOS 2024
İSTANBUL

T.C.
İSTANBUL GEDİK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

TÜRKİYE'DE FAALİYET GÖSTEREN DENİZ TAŞIMACILIĞI İŞLETMELERİNE YÖNELİK SİBER RİSK ANALİZİ İÇİN MATEMATİKSEL MODEL ÖNERİSİ

DOKTORA TEZİ

Saim Atalay KELEŞTEMUR
(181236002)
(0009-0006-5493-2112)

Uluslararası Ticaret Anabilim Dalı

Uluslararası Ticaret Doktora Programı

Tez Danışmanı: Prof. Dr. Süha ATATÜRE

İstanbul 2024

T.C.
İSTANBUL GEDİK ÜNİVERSİTESİ
Lisansüstü Eğitim Enstitüsü Müdürlüğü

Jüri Tez Onay Formu

29 Ağustos 2024

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ MÜDÜRLÜĞÜ

Bu çalışma 29 Ağustos 2024 tarihinde aşağıdaki jüri tarafından Uluslararası Ticaret ve Finansman Anabilim Dalı, Uluslararası Ticaret (Doktora) Programı Doktora Tezi olarak kabul edilmiştir.

TEZ JÜRİSİ

Prof. Dr. Süha ATATÜRE
Danışman
İstanbul Gedik Üniversitesi

Dr. Öğr. Üyesi Güldem ELMAS
Üye (İmza)
İstanbul Cerrahpaşa Üniversitesi

Prof. Dr. Mehmet Ziya SÖĞÜT
Üye (İmza)
Piri Reis Üniversitesi

Prof. Dr. Mehmet ERKAN
Üye (İmza)
İstanbul Gedik Üniversitesi

Dr. Öğr. Üyesi İsmail ÖZDEMİR
Üye (İmza)
İstanbul Gedik Üniversitesi

YEMİN METNİ

Doktora Tezi olarak sunduğum "Türkiye'de Faaliyet Gösteren Deniz Taşımacılığı İşletmelerine Yönelik Siber Risk Analizi İçin Matematiksel Model Önerisi" başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere uygun şekilde tarafımca yazıldığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmamın içinde kullanıldıkları her yerde bunlara atıf yapıldığını, patent ve telif haklarını ihlal edici bir davranışımın olmadığını belirtir ve bunu onurumla doğrularım (29.08.2024).

Saim Atalay KELEŞTEMUR

ÖNSÖZ

Türkiye'de faaliyet gösteren deniz taşımacılığı işletmelerinin etkin bir siber risk analizi yapabilmeleri için geliştirdiğim matematiksel model önerisini konu alan tez çalışmamda, tecrübeleriyle beni aydınlatan pek saygıdeğer tez danışmanım Prof. Dr. Süha ATATÜRE'ye teşekkürlerimi sunarım.

Tezin oluşum sürecindeki yardım, katkı ve motivasyonlarından dolayı tez jürimde bulunan Dr. Öğr. Üyesi Güldem ELMAS, Prof. Dr. Mehmet ERKAN, Prof. Dr. Ziya SÖĞÜT ve Dr. Öğr. Üyesi İsmail ÖZDEMİR'e çok teşekkür ederim.

Tez çalışmam süresince bana destek olan Prof. Dr. Mustafa ALKAN'a, Dr. Öğr. Üyesi Tayfun ACARER'e, Dr. Öğr. Üyesi Ümit BOZOKLU'ya ve Dr. Öğr. Üyesi Ahmet ERKASAP'a teşekkür ederim.

Ayrıca, tüm eğitim yaşamım boyunca hep yanımda olan, beni sürekli motive eden ve bana her şartta güvenen aileme, hiçbir koşulda elimi bırakmayan, gerek çalışma ortamı gerek moral ortamının oluşmasındaki yoğun katkısı ve desteğinden dolayı, sevgili eşime sonsuz teşekkür ederim.

Ağustos 2024 Saim Atalay KELEŞTEMUR

İÇİNDEKİLER

Sayfa No:

KISALTMALAR

AIS	**:**	Otomatik Tanımlama Sistemi
APT	**:**	Gelişmiş Kalıcı Tehdit
BGYS	**:**	Bilgi Güvenliği Yönetim Sistemleri
BIMCO	**:**	Baltık ve Uluslararası Denizcilik Konseyi
BT	**:**	Bilgi Teknolojileri
CAPEC	**:**	Ortak Saldırı Deseni Sayımı ve Sınıflandırması
CIA	**:**	Gizlilik, Bütünlük, Erişilebilirlik
DDoS	**:**	Dağıtık Hizmet Reddi Saldırısı
ECDIS	**:**	Elektronik Harita Gösterim ve Bilgi Sistemi
ETA	**:**	Olay Ağacı Analizi
FTA	**:**	Hata Ağacı Analizi
GNSS	**:**	Küresel Navigasyon Uydu Sistemleri
GPS	**:**	Küresel Konumlama Sistemi
IEC	**:**	Uluslararası Elektroteknik Komitesi
ILO	**:**	Uluslararası Çalışma Örgütü
IMO	**:**	Uluslararası Denizcilik Örgütü
INTERTANKO	**:**	Uluslararası Bağımsız Tanker Sahipleri Birliği
IoT	**:**	Nesnelerin İnterneti
ISMS	**:**	Uluslararası Güvenlik Yönetim Sistemleri
ISO	**:**	Uluslararası Standardizasyon Teşkilatı
ISPS	**:**	Uluslararası Gemi ve Liman Tesisi Güvenlik Kodu
MIoT	**:**	Denizcilikte Nesnelerin İnterneti
MLC	**:**	Denizcilik Çalışma Sözleşmesi
NSR	**:**	Kuzey Denizi Rotası
OWASP	**:**	Açık Web Uygulama Güvenliği Projesi
PFSP	**:**	Liman Tesisi Güvenlik Planı
PUKÖ	**:**	Planla, Uygula, Kontrol Et, Önlem Al
SOLAS	**:**	Denizde Can Güvenliği Uluslararası Sözleşmesi
SQLi	**:**	Structured Query Language Injection
SSP	**:**	Gemi Güvenlik Planı
VDR	**:**	Sefer Veri Kaydedici

ÇİZELGE LİSTESİ

Sayfa No:

ŞEKİL LİSTESİ

Sayfa No:

TÜRKİYE'DE FAALİYET GÖSTEREN DENİZ TAŞIMACILIĞI İŞLETMELERİNE YÖNELİK SİBER RİSK ANALİZİ İÇİN MATEMATİKSEL MODEL ÖNERİSİ

ÖZET

Denizcilik sektörü, küresel ticaretin yaklaşık %90'ını gerçekleştirmesi nedeniyle uluslararası ticaretin en kritik bileşenlerinden biridir. Denizcilik sektörüne ilişkin bilişim teknolojilerindeki gelişmenin hız kazanmasıyla birlikte gemi ve liman operasyonları, artan siber güvenlik tehditlerine maruz kalmaktadır. Bu tehditler, denizcilik operasyonlarını kesintiye uğratabilecek ve büyük maddi kayıplara yol açabilecek zafiyetler yaratmaktadır.

Bu çalışma, Türkiye'de faaliyet gösteren deniz taşımacılığı işletmelerine yönelik siber risklerin değerlendirilmesi ve bu risklere karşı bir matematiksel model geliştirilmesi amacıyla yapılmıştır. Çalışmada, siber saldırıların gemilere ve denizcilik operasyonlarına olan etkilerini anlamak ve azaltmak için MITRE CAPEC saldırı vektörleri ve Monte Carlo simülasyonu kullanılmıştır.

Gemi sistemlerindeki siber riskler, nitel ve nicel analizleri birleştiren hibrit bir modelle ele alınmış, risklerin etkisi ve olasılığı detaylı bir şekilde incelenmiştir. Bu analizler sonucunda, siber güvenlik bütçelerinin en etkin şekilde kullanılması ve kritik risklerin önceliklendirilmesi için Optimum Maliyet Dengesi Algoritması geliştirilmiştir. Bu algoritma, sınırlı kaynaklar doğrultusunda en yüksek riske sahip zafiyetlerin azaltılmasına olanak tanımaktadır.

Geliştirilen risk analiz çerçevesi, sadece Türkiye'deki deniz taşımacılığı sektörüne değil, aynı zamanda küresel denizcilik sektörüne de uygulanabilir bir yapıdadır. Çalışmanın sonunda, denizcilik sektöründeki siber güvenlik tehditlerinin daha sistematik bir şekilde yönetilmesi ve sektördeki paydaşların siber güvenlik farkındalığının artırılması hedeflenmiştir.

Ayrıca, bu çerçevenin denizcilik dışındaki sektörlerde de kullanılabilecek esnekliğe sahip olması, araştırmanın literatüre katkısını güçlendirmektedir.

Anahtar Kelimeler: *Denizcilik, Siber Güvenlik, Risk Analizi, Monte Carlo Simülasyonu, Optimum Maliyet Dengesi*

A MATHEMATICAL MODEL PROPOSAL FOR CYBER RISK ANALYSIS OF MARITIME TRANSPORT COMPANIES OPERATING IN TURKEY

ABSTRACT

The maritime sector is one of the most critical components of international trade, as it accounts for approximately 90% of global trade. With the rapid development of information technologies in the maritime sector, ship and port operations are increasingly exposed to cybersecurity threats. These threats create vulnerabilities that could disrupt maritime operations and lead to significant financial losses.

This study aims to assess the cyber risks facing maritime transport companies operating in Turkey and to develop a mathematical model to address these risks. MITRE CAPEC attack vectors and Monte Carlo simulations have been used to understand and mitigate the effects of cyberattacks on ships and maritime operations.

Cyber risks in ship systems have been analyzed using a hybrid model that combines qualitative and quantitative methods, with a detailed examination of the impact and likelihood of these risks. As a result of this analysis, the Optimum Cost Balance Algorithm was developed to ensure the most efficient use of cybersecurity budgets and to prioritize the mitigation of critical risks. This algorithm allows for the reduction of vulnerabilities with the highest risk, considering limited resources.

The developed risk analysis framework is applicable not only to the maritime transport sector in Turkey but also to the global maritime industry. At the conclusion of the study, it is expected that cybersecurity threats in the maritime sector will be managed more systematically, and stakeholders' cybersecurity awareness will be enhanced.

Additionally, the flexibility of this framework to be used in sectors outside of maritime further strengthens the study's contribution to the literature.

Keywords: *Maritime, Cybersecurity, Risk Analysis, Monte Carlo Simulation, Optimum Cost Balance*

1. GİRİŞ

Deniz taşımacılığı, uluslararası ticaretin önemli bir bileşenidir ve küresel ekonomi için hayati bir bağlantı görevi görmektedir. Bu da sınır ötesi ticareti kolaylaştırmadaki önemli rolünü vurgulamaktadır (Cuong vd., 2020). Denizcilik endüstrisindeki altyapının verimliliği ve gelişimi, ülkelerin uluslararası ticaret alanındaki rekabet gücünü artırmada anahtar faktörlerdir. Ülkelerin sürdürülebilir ekonomik kalkınması, deniz taşımacılığının uluslararası ticareti desteklemedeki vazgeçilmez rolü ile yakından bağlantılıdır (Xu vd., 2020).

Uluslararası deniz ticareti hacmi, son yüzyılda istikrarlı bir şekilde artmış olup, şu anda dünya ticaretinin yaklaşık yüzde 90'ı deniz yoluyla gerçekleştirilmektedir. Limanlar, deniz taşımacılığının hayati bileşenleri olarak, dünya ticaret akışlarının önemli bir bölümünü işleyen uluslararası ticaret ağındaki kritik düğümler olarak hizmet vermektedir (Blonigen ve Wilson, 2007). Sürdürülebilir deniz taşımacılığının stratejik önemi, 2030 Sürdürülebilir Kalkınma Ajandası ve Paris Anlaşması'nda belirtilen küresel sürdürülebilirlik hedeflerine ulaşmaya katkıda bulunmayı amaçlamaktadır.

Deniz taşımacılığı altyapısına yapılan yatırımların ihracatı teşvik ettiği, ticaret akışlarını artırdığı ve deniz ticareti hacimlerini artırdığı gösterilmiştir. Uluslararası ticaretin büyümesiyle, deniz taşımacılığının rolü daha da kritik hale gelmekte olup, küresel ticaretin birbirine bağlı manzarasında önemini vurgulamaktadır (Yıldız, 2022).

Denizcilik riskleri, denizcilik endüstrisinin güvenliği, emniyeti ve operasyonları için önemli tehlikeler oluşturan geniş bir tehdit ve zorluk yelpazesini kapsamaktadır. Bu riskler, korsanlık ve deniz terörizmi gibi geleneksel sorunlardan siber tehditler ve çevresel suçlar gibi ortaya çıkan tehditlere kadar uzanmaktadır (Karamperidis vd., 2021). Geniş gemi, liman ve tedarik zinciri ağı ile denizcilik sektörü, operasyonları kesintiye uğratmak ve zarar vermek isteyen kötü niyetli aktörler tarafından istismar edilebilecek zafiyetler yaratmaktadır (Balduzzi vd., 2014).

Siber güvenlik alanında, denizcilik operasyonlarında dijital teknolojilere artan bağımlılık, endüstriyi denizcilik sistemlerinin güvenliğini ve bütünlüğünü tehlikeye atabilecek siber tehditlere maruz bırakmıştır. Otomatik Tanımlama Sistemi (AIS) gibi sistemlerdeki zafiyetler ve otonom gemilere yönelik siber saldırı potansiyeli, veri ihlallerine ve operasyonel kesintilere karşı koruma sağlamak için sağlam siber güvenlik önlemlerinin gerekliliğinin altını çizmektedir.

Uluslararası Güvenlik Yönetim Sistemleri (ISMS), Gemi Güvenlik Planı (SSP) ve Uluslararası Gemi ve Liman Tesisi Güvenlik (ISPS) Kodu, küresel denizcilik operasyonlarının güvenliğini ve emniyetini sağlamak için önemli bileşenlerdir. ISPS Kodu, Uluslararası Denizcilik Örgütü (IMO) tarafından 2004 yılında küresel korsanlık ve terör tehditlerine yanıt olarak oluşturulmuştur. Bu kod, hükümetler, gemi donatanları ve liman tesisleri arasında gemilere ve limanlara yönelik güvenlik tehditlerini belirlemek, değerlendirmek ve yanıt vermek için uluslararası işbirliğini teşvik etmektedir (Radonja ve Glujić, 2020).

ISPS Kodu'na göre, her gemi bir Gemi Güvenlik Planı'na sahip olmalıdır. SSP, uluslararası ticarete dahil olan gemileri etkileyen güvenlik olaylarını önlemek için gemide uygulanacak güvenlik prosedürlerini ve önlemlerini açıklamaktadır (Grapa ve Lemoncito, 2021). ISPS Kodu ayrıca, hükümetlerin, gemi şirketlerinin, gemi personelinin ve liman tesisi personelinin güvenlik tehditlerini tespit etmek ve güvenlik olaylarına karşı önleyici tedbirler almak için işbirliği yapmasını gerektirir. Denizcilik sektöründe ortaya çıkan siber tehditler, gemiler için özel olarak uyarlanmış siber risk çerçevelerini uygulayarak geliştirilebilecek Gemi Siber Güvenlik Planı'nın gerekliliğini öne çıkarmaktadır.

Bu tez çalışması, gemilerdeki siber risklerin önemini ortaya koymaktadır. MITRE CAPEC, yaygın saldırı kalıplarının bir kataloğu kullanılarak genişletilen ve uygulanan bir siber risk değerlendirme metodolojisi ile literatüre katkıda bulunmayı amaçlamaktadır. Her saldırı kalıbı, IMO tarafından yayınlanan Denizcilik Siber Risk Yönetimi Kılavuzlarına göre sınıflandırılmıştır. MITRE CAPEC üzerinden deniz taşımacılığına yönelik filtrelenen riskler, daha sonra Monte Carlo yöntemi ile matematiksel bir risk analiz sonucu sunmaktadır.

1.1. Araştırmanın Problemi

Araştırmanın problemi; denizcilik sektörünü etkileyen siber güvenlik faaliyetlerinin hangi saldırı vektörlerinin kullanılarak yapılmakta, bu saldırıların olasılıkları, şiddetleri ve etkileri nedir? Siber güvenlik için ayrılan bütçeyi, nasıl en etkin şekilde kullanarak risk iyileştirme faaliyetlerini gerçekleştirilebilir? sorularına yanıt bulmaktadır. Bu kapsamda çalışma, olası saldırıların direkt etkilerini senaryo tabanlı bir sistematik üzerinden ölçümlemek ve çözümleyen bir çerçeve sunmaktadır. Bu çerçevenin denizcilik sektörünün, işletmelerin bütçesi doğrultusunda siber güvenlik pozisyonunu azami ölçüde güçlendirmesine yardımcı olacağı öngörülmektedir.

1.2 Araştırmanın Amacı ve Önemi

Siber güvenlik konusu son yıllarda gerek akademik camia gerekse de iş dünyası için önemli bir konu haline gelmiştir. Gelişen siber saldırılar neticesinde irili ufaklı birçok firma veri hırsızlığına maruz kalmış, hizmet veremez hale gelmiş ve tüm bu vakalar neticesinde büyük ölçüde finansal kayıplar yaşamıştır. Siber saldırılara karşı geliştirilen siber güvenlik çözümleri tek başına yeterli olmamaktadır. Derinlemesine savunma sağlayabilmek için işletmelerin bilgi güvenliği yönetim sistemlerini oluşturması; buna bağlı olarak, saldırı vektörlerini tanıması, risk analizi yapması ve gerekli siber güvenlik önlemlerini alması gerekmektedir.

Gelişen teknolojiye uyum göstermesiyle birlikte, denizcilik sektörü de siber saldırılardan en çok etkilenen sektörlerden biri haline gelmiştir. Bunun temel sebepleri, sektörde bulunan paydaşların siber güvenlik disiplininin az olması, gemi üretimi sırasında kullanılan elektronik donanımın güvenlik standartlarına uygun olmaması ve her geçen gün daha fazla bilgisayar destekli hale gelen gemi köprü üstü seyir ve makine/pervane sistemleri gösterilebilir.

Literatür incelendiğinde, denizcilik sektörünü olumsuz etkilemiş, çeşitli siber güvenlik vakasının bulunduğu görülmektedir. Bu siber saldırılar, operasyonel faaliyetleri durdurmuş, yük bilgisine erişimi engellemiş, gemilerdeki köprü üstü sistemler ile makine/pervane sistemlerini çalışamaz hele getirmiş, seyir emniyetini tehlikeye sokmuş ve hatta çatışmalara sebep olmuştur. Tüm bunlar neticesinde denizcilik işletmeleri finansal açıdan da önemli kayıplar yaşamıştır. Bununla birlikte

özellikle IMO başta olmak üzere INTERTANKO ve BIMCO gibi örgütler siber güvenliğin önemine değinmiş ve konuyla ilgili ekler, yönergeler, bildiriler yayınlamıştır.

Denizcilik sektöründe siber güvenlikle ilgili çeşitli araştırmalar yapılmasına rağmen, henüz ortaya olgunlaşmış, özellikle de matematiksel bir modele dayalı çerçeve bulunmamaktadır. Mevcut risk analiz çerçevelerine ilişkin yapılan akademik araştırmalar ise yeterli değildir. Gelişen teknoloji ve buna bağlı olarak sürekli artan siber saldırıların, denizcilik sektörünü daha fazla etkilememesi için, tüm paydaşların kullanabileceği, özellikle de gemi mürettebatına bir kontrol listesi niteliği taşıyabilecek küresel bir çerçevenin oluşturulması önemlidir.

Çalışma kapsamında denizcilik sektörünü hedef alan siber saldırıların olası etkilerinin araştırılması hedeflenmektedir. Çalışmanın bir diğer amacı ise az sayıdaki yaşanmış vakaları senaryo simülasyonları üzerinden olgunlaştırmak ve buna göre gerekli koruyucu güvenlik önemlerini sunmaktır. Denizcilik işletmeleri açısından yeni sayılabilecek siber güvenlik konusu için ayrılması gereken bütçenin öngörülmesi ve bütçe üzerinden hangi risklerin öncelikli olarak kapatılması konusunda işletmelere yardımcı olmak da bir diğer önemli amaçtır. Bu bağlamda yaşanmış tüm vakalar incelenmiş, gemiler için risk envanteri oluşturulmuş ve hibrit bir risk analiz modeli oluşturulmuştur.

Çalışma denizcilik sektörü kapsamında çerçevelenmiştir. Bununla birlikte çerçevenin altyapısını oluşturan model, farklı sektörlerde de kullanılabilmesi için esnek tutulmuştur. Model oluşturulurken MITRE CAPEC saldırı vektörleri ve Monte Carlo simülasyonu ele alınmıştır.

Araştırmaya özgün değer katan ve onu bu alanda önemli kılan konu ise nitel ve nicel risk analiz yöntemlerini birleştirerek oluşturulan hibrit modeldir. Bu hibrit model sayesinde risk analizini yapan kişi ya da kurumların öngörü becerisinden başka, matematiksel bir senaryo oluşturma modeli ile gerçeğe yakın sonuçlar elde edilebilmektedir. Araştırma sonucunda elde edilen veriler, bu veriler kullanılarak oluşturulan risk envanteri ve çerçevenin denizcilik sektörüne katkı sağlaması beklenmektedir.

Ayrıca çalışma, denizcilik sektörü için geliştirilmiş hibrit bir risk analiz modeli olması sebebiyle de literatürdeki ilk çalışma olması dolayısıyla da öneme sahiptir.

1.3 Araştırmanın Sınırlılıkları

Araştırma sınırlılıkları, çalışmanın kapsamını, örneklem büyüklüğünü, kullanılan yöntemleri ve elde edilen verilerin yorumlanmasını etkilemektedir. Örneğin, Kolcu'nun çalışmasında, Covid-19 korkusunun aşılanmaya etkisi incelenmiş ve araştırmanın yalnızca İstanbul'da gerçekleştirilmiş olması, sonuçların genellenebilirliğini sınırlamaktadır (Kolcu, 2023).

Araştırma sınırlılıkları, aynı zamanda araştırmanın metodolojik yapısını da etkilemektedir. Algılanan sosyal destek ile sağlıklı yaşam davranışları arasındaki ilişki incelenirken, belirli bir örneklem grubunun seçilmesi, sonuçların genellenebilirliğini kısıtlamaktadır (Kanığ, 2020). Bu tür sınırlamalar, araştırmanın bulgularının güvenilirliğini sorgulatabilir ve araştırmacıların daha geniş bir örneklem üzerinde çalışmalarını teşvik edebilmektedir.

Çalışmanın verileri, zaman kısıtı ve örnekleme belirleme zorluğu sebebiyle, kolayda örnekleme yöntemi kullanılarak 2000 ila 2024 yılları arasındaki siber vakaları kapsamaktadır. Araştırmada veri toplama aracı olarak literatür taraması yapılmış olup, denizcilik sektöründe yaşanmış siber saldırılar incelenerek, saldırı vektörleri tespit edilmiştir. Elde edilen saldırı vektörleri MITRE CAPEC ID'ler ile eşleştirilerek, başta gemiler olmak üzere, siber uzay içinde yer alan tüm tesislerine yönelik gerçekleşmesi olası siber saldırılara yönelik risk analizi yapılmasına yardımcı olmaktadır.

Araştırma, Türk denizcilik sektöründe faaliyet gösteren işletmelere ait gemilerden oluşan örneklem ile sınırlıdır. Ancak gemilerde kullanılmakta olan bileşenler uluslararası deniz filosu ile büyük ölçüde benzerlik gösterdiğinden, çerçeveyi kullanarak herhangi bir gemiye ait risk analizi yapılabileceği öngörülmektedir. MITRE CAPEC ID'ler, bilgisayar destekli gemi sistemlerine yönelik seçilmiş ve risk envanterine eklenmiştir. Oluşturulan çerçeve, matematiksel bir model üzerine inşa edilmiş olup, tüm denizcilik paydaşlarınca, gemi dışı bileşenler için de kullanılabilir.

Araştırmanın bulguları ve çıkarılan sonuçlar, yürütülen araştırma evreni ile sınırlıdır.

1.4 Araştırmanın Etik Boyutu

Çalışma kapsamında ölçme aracının oluşumunu sağlayan ölçekler, uluslararası siber güvenlik standartları ve çerçeveleri kullanılarak çalışma kapsamına dahil edilmiştir.

Çalışmanın örneklem grubunun üzerinde uygulanabilmesi için gemi bileşenlerine gerçek saldırılardan kaçınılmış, laboratuvar ortamında simüle edilmiştir. Ayrıca yaşanmış vakalar incelenmiş ve saldırı vektörleri analiz edilmiştir.

Tüm süreç, Monte Carlo simülasyonu yöntemi ile olgunlaştırılarak, gerçeğe yakın sonuçların elde edilmesine çalışılmıştır.

Kaynaklara doğru şekilde atıf yapılmasına dikkat edilmiştir.

2. KAVRAMSAL ÇERÇEVE/GENEL BİLGİLER

Bu çalışmanın temelini oluşturan matematiksel risk analiz modeli, siber güvenlik, bilgi güvenliği, bilgi güvenliği yönetim sistemleri, denizcilik sektörü, risk analizi ve risk yönetimi gibi çeşitli temel kavramlar üzerine inşa edilmiştir. Her bir kavramın çalışmayla olan ilişkisi doğrultusunda, bu kavramların ne anlama geldiğinin ifade edilmesi, tarihsel gelişim süreçlerinin ele alınması, yaşanmış vakaların analiz edilmesi ve koruyucu güvenlik süreçlerinin incelenmesi büyük önem taşımaktadır.

2.1. Bilgi Güvenliği

Bilgi güvenliği, bilgi ve bilgi sistemlerinin yetkisiz erişim, ifşa, kesinti, değişiklik veya imhadan korunmasına odaklanan kritik bir disiplindir. Hassas verileri korumak ve gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için tasarlanmış çok çeşitli uygulamaları, teknolojileri ve politikaları kapsar; genellikle CIA (Confidentiality, Integrity, Availability/Gizlilik, Bütünlük, Erişilebilirlik) üçlüsü olarak anılır (Liu vd., 2020). Bu temel çerçeve, giderek dijitalleşen bir dünyada sağlam güvenlik önlemleri oluşturmak isteyen işletmeler için yol gösterici bir ilke görevi görmektedir.

Bilgi güvenliği kavramı, salt teknik çözümlerin ötesine uzanır; insanları, süreçleri ve teknolojiyi entegre eden bütünsel bir yaklaşımı içerir. Bilgi güvenliği için kapsamlı bir çerçeve toplumsal eğilimleri, insan unsurlarını ve değişen teknolojilerin karmaşıklıklarını dikkate almalıdır. Bu bakış açısı, kuruluşların insan davranışı ve karar alma ile ilişkili riskleri önemli ölçüde azaltabilen güçlü bir bilgi güvenliği kültürü oluşturma ihtiyacını vurgulamaktadır (Veiga vd., 2020). Böyle bir güvenlik kültürü geliştirmenin önemi, iyi tanımlanmış bir bilgi güvenliği yönetiminin tehditleri en aza indirebileceğini ve veri ihlali olaylarını azaltabileceğini gösteren araştırmalarla daha da desteklenmektedir.

Bilgi güvenliği farkındalığının ölçülmesi etkili yönetim için çok önemlidir. Güvenlik farkındalığı programları, bir işletme içindeki bireylerin bilgi ve becerilerini

geliştirmek ve böylece genel güvenlik duruşunu iyileştirmek için tasarlanmıştır. Bu programlar, belirli bilgi güvenliği alanlarını ele alacak şekilde düzenlenmeli ve etkinliklerini değerlendirmek için uygun ölçüm yöntemleri kullanılmalıdır. Farkındalık ve güvenlik politikalarına uyum arasındaki etkileşim, hayati önem taşımaktadır ve çalışanların davranışları, işletmelerin güvenlik ortamını doğrudan etkilemektedir (Erick vd., 2019). Bu ifade, insan faktörünün bilgi güvenliği açısından önemini vurgulamaktadır.

Bilgi güvenliğinin yönetimi, ticari işletmelerin ele alması gereken bir diğer kritik husustur. Tehditlerin gelişen doğası, işletmelerin değişen güvenlik ortamlarına uyum sağlayabilen dinamik yönetim çerçeveleri benimsemesini gerektirmektedir. Bu gereksinim, hedeflenen güvenlik seviyelerini ve uyumluluk gerekliliklerini ifade eden net güvenlik politikaları oluşturmayı içermektedir. Etkili yönetişim yalnızca politikalar belirlemekle kalmaz, aynı zamanda bu politikaların kuruluş genelinde iletilmesini ve uygulanmasını da kapsamaktadır.

Yönetişim ve güvenlik kültürüne ek olarak, bilgi güvenliğinin teknik yönleri göz ardı edilmemelidir. Şifreleme, erişim kontrolleri ve saldırı tespit sistemleri gibi güvenlik önlemlerinin uygulanması, hassas bilgileri yetkisiz erişimden ve ihlallerden korumak için elzemdir (Vuorinen ve Tetri, 2012). Gizlilik ve bütünlük arasındaki etkileşimi anlamak, etkili güvenlik stratejileri geliştirmek için çok önemlidir. İşletmeler, kapsamlı güvenlik politikaları formüle etmek için saldırganların bu iki boyut üzerindeki potansiyel etkilerinin farkında olmalıdır.

2.1.1 Gizlilik, bütünlük, erişilebilirlik üçgeni

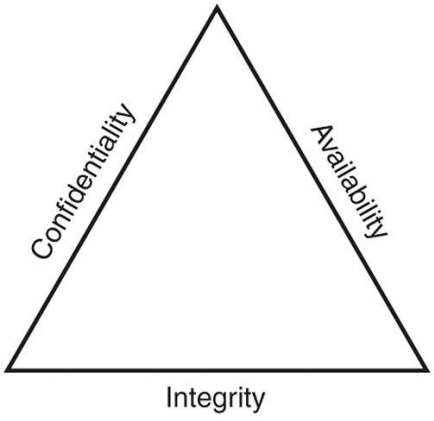
Gizlilik, Bütünlük ve Erişilebilirlik anlamına gelen CIA üçlüsü, bilgi güvenliği alanında temel bir modeldir. Bu üçlü, kuruluşların hassas bilgileri çeşitli tehditlerden korumak için etkili güvenlik politikaları ve uygulamaları geliştirmeleri ve uygulamaları için bir rehber ilke görevi görmektedir. Üçlünün her bir bileşeni, bilgi sistemlerinin güvenli ve verimli bir şekilde çalışmasını sağlamada kritik bir rol oynamaktadır.

Gizlilik, bilgilerin yetkisiz erişim ve ifşadan korunmasını ifade eder. Hassas verilere yalnızca uygun izinlere sahip kişiler veya sistemler tarafından erişilebilmesini sağlar. Gizliliğin korunması, kimlik hırsızlığına, mali kayba veya itibar kaybına yol açabilecek ihlallere karşı kişisel ve kurumsal verileri korumak için

esastır. Şifreleme, erişim kontrolleri ve kimlik doğrulama mekanizmaları gibi teknikler gizliliği korumak için yaygın olarak kullanılır. Gizliliğin önemi, bu alandaki herhangi bir uzlaşmanın yasal sonuçlar ve müşteri güveninin kaybı dahil olmak üzere ciddi sonuçlara yol açabileceği gerçeğiyle vurgulanmaktadır (Crihan vd., 2023).

Bütünlük, bilgilerin doğruluğunu ve eksiksizliğini korumayı içerir. Verilerin yetkisiz kişiler tarafından değiştirilmemesini veya kurcalanmamasını sağlar. Bütünlük, yanlış bilgiye veya operasyonel kesintilere yol açabilecek yetkisiz değişiklikleri önlemede kritik öneme sahiptir. İşletmeler, yetkisiz değişiklikleri tespit etmeye yardımcı olan kontrol toplamları, karma işlevleri ve denetim izleri dahil olmak üzere veri bütünlüğünü sağlamak için çeşitli önlemler uygular (Nair, 2016). Bütünlüğün önemi, özellikle veri doğruluğunun karar alma ve düzenleyici standartlara uyum için çok önemli olduğu finans, sağlık hizmetleri ve denizcilik gibi sektörlerde belirgindir.

Erişilebilirlik, bilgi ve kaynakların yetkili kullanıcılar tarafından gerektiğinde erişilebilir olmasını sağlar. CIA üçlüsünün bu yönü, iş sürekliliğini ve operasyonel verimliliği korumak için oldukça önemlidir. Erişilebilirlik donanım arızaları, siber saldırılar ve doğal afetler dahil olmak üzere çeşitli faktörler tarafından tehdit edilebilir. İşletmeler, erişilebilirliği artırmak ve kesinti süresini en aza indirmek için yedeklilik, devralma sistemleri ve düzenli yedeklemeler uygulamalıdır. Dijital hizmetlere ve bulut bilişimine artan bağımlılık, kritik bilgilere kesintisiz erişimi desteklemek için sağlam erişilebilirlik önlemlerine olan ihtiyacı daha da vurgulamaktadır (Lopes ve Oliveira, 2016).



Şekil 2.1: Gizlilik, Erişilebilirlik, Bütünlük Üçgeni

CIA üçlüsü bileşenleri birbirine bağımlıdır; bir alandaki bir uzlaşma diğerlerini önemli ölçüde etkileyebilir. Örneğin, gizlilik ihlal edilirse, yetkisiz kullanıcılar tespit edilmeden bilgileri değiştirebileceğinden verilerin bütünlüğü de sorgulanabilir. Benzer şekilde, bir hizmet reddi saldırısı (DoS) nedeniyle kullanılabilirlik tehlikeye girerse, veri bütünlüğünü ve gizliliğini koruma yeteneği engellenebilir. Bu nedenle kuruluşların bu üç bileşeni aynı anda ele alan bütünsel bir güvenlik yaklaşımı benimsemeleri gerekmektedir.

2.1.2 Bilgi güvenliği ve siber güvenlik arasındaki farklar

Dijital koruma alanında, "bilgi güvenliği" ve "siber güvenlik" terimleri sıklıkla birbirinin yerine kullanılır, ancak farklı kavramları ve uygulamaları kapsar. Bu iki alan arasındaki farkları anlamak, verilerini ve sistemlerini etkili bir şekilde korumayı amaçlayan kuruluşlar için çok önemlidir. Bilgi güvenliği, dijital, fiziksel veya fikri olsun, her türlü bilgiyi korumaya odaklanan geniş bir nosyondur. Hassas verileri yetkisiz erişim, ifşa, değişiklik ve imhadan korumak için tasarlanmış politikaları, prosedürleri ve teknolojileri kapsamaktadır.

Çizelge 2.1: Bilgi Güvenliği ve Siber Güvenlik Arasında Karşılaştırma

Kriter	Bilgi Güvenliği	Siber Güvenlik
Odak Noktası	Bilginin her türlü yetkisiz erişimden, ifşadan ve değişiklikten korunması.	Bilgisayar sistemlerinin, ağların ve dijital verilerin siber tehditlerden korunması.
Kapsam	Dijital, fiziksel ve fikri bilgi korunmasını kapsar.	Özellikle dijital ortam ve siber uzay üzerindeki tehditlere karşı korunmayı içerir.
Tehdit Türleri	Fiziksel saldırılar, veri sızıntıları, iç tehditler.	Kötü amaçlı yazılımlar, DDoS saldırıları, kimlik avı saldırıları.
Koruma Yöntemleri	Şifreleme, erişim kontrolü, güvenlik politikaları, fiziksel güvenlik.	Güvenlik duvarları, antivirüs yazılımları, saldırı tespit sistemleri, ağ izleme vb.
Yönetmelikler ve Standartlar	GDPR, HIPAA, PCI DSS vb. düzenlemeler.	NIST Siber Güvenlik Çerçevesi, OWASP Test Kılavuzu vb.
Teknoloji Kullanımı	Fiziksel ve dijital bilgi güvenliği teknolojilerini kapsar (şifreleme, erişim kontrolü vb).	Yalnızca dijital sistemlerin ve siber uzayın güvenliğini sağlamaya odaklanır.

Bilgi güvenliği, bir kuruluş içinde güvenlik açıklarını ele alan ve güvenlik seviyelerini artırmak için karşı önlemler uygulayan çok çeşitli alanları içerir. Gizlilik, Bütünlük ve Erişilebilirlik üçlüsü bilgi varlıklarını korumak için yol gösterici bir çerçeve görevi görmektedir (Thirumaran vd., 2010). Siber güvenlik ise özellikle bilgisayar sistemlerinin, ağların ve dijital verilerin siber tehditlerden korunmasıyla

ilgili faaliyetler bütünüdür. Teknolojideki ve internetteki güvenlik açıklarından yararlanan saldırılara karşı savunmaya odaklanır.

Siber güvenlik, bilgilerin paylaşıldığı ve ifşa edildiği daha geniş siber uzay bağlamını göz önünde bulundurarak bir işletmenin sınırlarının ötesine uzanır. Bu ayrım, tüm siber güvenlik önlemlerinin, bilgi güvenliğinin bir parçası olmasına rağmen, tüm bilgi güvenliği önlemlerinin siber güvenlikle ilgili olmadığını vurgulamaktadır (Gcaza ve Solms, 2017). Bilgi güvenliği ve siber güvenlik arasındaki farklar, temel olarak dört başlık altında toplanabilir.

2.1.2.1 Odak ve kapsam

Bilgi güvenliği, dijital korumalara ek olarak fiziksel güvenlik, personel güvenliği ve operasyonel güvenliği içeren daha geniş bir koruyucu önlem yelpazesini kapsamaktadır. Siber güvenlik, esas olarak dijital varlıkları ve bunları destekleyen altyapıyı korumakla ilgilenir (Frisk vd., 2023). Bu çalışmalar, ağları, sunucuları ve uygulamaları kötü amaçlı yazılım, kimlik avı ve hizmet reddi saldırıları gibi siber tehditlerden korumayı içerir.

2.1.2.2 Tehdit yapısı

Bilgi güvenliğinin ele aldığı tehditler, bilgilere fiziksel erişim, içeriden gelen tehditler ve veri ihlalleri ile ilişkili riskler de dahil olmak üzere hem dijital hem de dijital olmayan unsurlar olabilir. Buna karşılık, siber güvenlik, bilgisayar korsanlığı girişimleri ve siber casusluk gibi internetten veya dijital ortamlardan kaynaklanan tehditlere odaklanır (Bailetti ve Craigen, 2020). Bu ayrım, her alanda kullanılan stratejileri ve teknolojileri etkilediği için önemlidir.

2.1.2.3 Düzenleyici ve uyumluluk yönleri

Bilgi güvenliği genellikle GDPR, HIPAA ve PCI-DSS gibi hassas verilerin korunmasını yöneten çeşitli düzenlemelere ve standartlara uyumu içerir. Bu düzenlemeler, fiziksel güvenlik önlemleri ve çalışan eğitimi dahil olmak üzere daha geniş bir kapsamı kapsayabilir. Siber güvenlik düzenlemeleri ise dijital varlıkları güvence altına almak için teknik standartlara ve protokollere daha fazla odaklanma eğilimindedir (Stevens, 2019).

2.1.2.4 Kültürel ve davranışsal boyutlar

Bilgi güvenliğini çevreleyen kültür, genellikle güvenli bir ortamı teşvik etmek için kurumsal politikaların, çalışan eğitiminin ve farkındalık programlarının önemini vurgulamaktadır. Bir işletme içindeki bilgi güvenliği kültürü, çalışanların bilgileri nasıl ele aldığını ve güvenlik protokollerine nasıl uyduğunu şekillendirir. Öte yandan siber güvenlik kültürü, siber tehditler bağlamında dijital bilgileri ve sistemleri koruyan davranışlara ve uygulamalara daha fazla odaklanır (Veiga, 2016).

2.1.3 Bilgi güvenliği yönetim sistemleri

Bilgi Güvenliği Yönetim Sistemleri (BGYS), kuruluşlar içindeki hassas bilgileri yönetmek ve korumak için tasarlanmış yapılandırılmış çerçevelerdir. Bilgi varlıklarının gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamayı amaçlayan kapsamlı bir politika, prosedür ve kontrol kümesini kapsamaktadır. BGYS'nin uygulanması, bilgi güvenliği ihlalleriyle ilişkili riskleri azaltmayı ve düzenleyici gerekliliklere uymayı amaçlayan işletmeler için hayati öneme sahiptir.

BGYS, hassas şirket bilgilerini yönetmeye yönelik sistematik bir yaklaşım olarak tanımlanabilir ve güvenliğinin insanlar, süreçler ve teknoloji kombinasyonuyla sağlanmasıdır. BGYS yalnızca teknik bir çözüm değil, bilgi güvenliğini kurumsal hedefler ve kurumsal yönetimle uyumlu hale getiren stratejik bir girişimdir. Bu uyum, bir güvenlik farkındalığı kültürü oluşturmak ve bilgi güvenliğinin kuruluşun tüm seviyelerinde bir öncelik olarak ele alınmasını sağlamak için önemlidir.

BGYS'nin temel amacı, bilgi güvenliğine yönelik riskleri etkili bir şekilde belirlemek ve yönetmektir. Bu kapsam, olası tehditleri, güvenlik açıklarını ve bilgi varlıkları üzerindeki etkileri değerlendirmeyi ve bu riskleri azaltmak için uygun kontrolleri uygulamayı içerir. Etkili bir BGYS yalnızca teknik yönleri değil, aynı zamanda bilgi güvenliğine katkıda bulunan işletmeye yönelik süreçleri ve insan faktörlerini de ele alır (Zammani vd., 2021).

Çizelge 2.2: Bilgi Güvenliği Yönetim Sistemi Bileşenleri

Bileşenler	Açıklama
Risk Yönetimi	Bilgi varlıklarına yönelik potansiyel tehditlerin tespiti, analiz edilmesi ve azaltılması.
Güvenlik Politikaları	İşletmenin bilgi güvenliğini sağlamak için geliştirdiği kurallar ve prosedürler.
Eğitim ve Farkındalık	Çalışanların güvenlik politikaları ve tehditler konusunda eğitilmesi ve bilinçlendirilmesi.
Olay Yönetimi	Güvenlik ihlallerine hızlı ve etkili müdahale için prosedürlerin belirlenmesi.
Varlık Yönetimi	Bilgi varlıklarının envanterinin çıkarılması ve bu varlıkların güvenliğinin sağlanması.
Uyumluluk ve Denetim	Mevzuat, yasal gereklilikler ve iç standartlarla uyumluluğun sağlanması ve denetlenmesi.
Sürekli İyileştirme	Güvenlik önlemlerinin ve politikalarının sürekli olarak gözden geçirilip, geliştirilmesi.

İşletmelere etkin bir BGYS kurmak için en yaygın olarak kabul gören standartlardan biri ISO/IEC 27001'dir. Bu uluslararası standart, işletmelerin bilgi güvenliği yönetim sistemlerini geliştirmeleri, uygulamaları, sürdürmeleri ve sürekli olarak iyileştirmeleri için bir çerçeve sağlar. Standart, bilgi güvenliği risklerini belirlemeyi, bunların potansiyel etkilerini değerlendirmeyi ve bunları azaltmak için kontroller uygulamayı içeren bir risk yönetimi sürecini ana hatlarıyla belirtir.

ISO/IEC 27001'e ek olarak, kuruluşların etkili BGYS uygulamasında rehberlik etmek için çeşitli diğer çerçeveler ve en iyi uygulamalar mevcuttur. Bunlar arasında COBIT, NIST, ITIL vb. yönergeler yer almaktadır (Mataracioglu ve Özkan, 2011). Bu çerçevelerin her biri, kuruluşların bilgi güvenliği risklerini sistematik bir şekilde yönetmelerine yardımcı olmak için belirli metodolojiler ve araçlar sunar. Etkili bir ISMS, çeşitli temel bileşenden oluşmaktadır.

2.1.3.1 Risk değerlendirmesi ve yönetimi

İşletmeler, bilgi varlıklarına yönelik potansiyel tehditleri ve güvenlik açıklarını belirlemek ve bunlara karşı etkili önlemler almak amacıyla düzenli olarak risk değerlendirmeleri yapmalıdır. Bu süreç, işletmenin sahip olduğu dijital ve fiziksel bilgi varlıklarını korumak için kritik bir adım olup, yalnızca mevcut tehditlerin tespit edilmesini değil, aynı zamanda bu tehditlerin gerçekleşme olasılıklarının ve potansiyel etkilerinin kapsamlı bir şekilde değerlendirilmesini de içerir.

Risk değerlendirmesi, olası risklerin hem kısa vadede hem de uzun vadede işletme üzerindeki etkilerini anlamayı amaçlar ve bu etkilerin maliyet, operasyonel süreklilik ve itibari kayıpları gibi faktörlere nasıl yansıyacağını analiz eder. Bu analiz, işletmenin hangi risklerin daha öncelikli olarak ele alınması gerektiğini belirlemesine yardımcı olmaktadır. Böylece kaynaklar en etkin şekilde kullanılabilir ve en yüksek öneme sahip tehditler öncelikli olarak azaltılabilir.

Risk değerlendirmesi ve yönetimi, işletmelerin karşılaşabileceği potansiyel tehlikeleri belirleme, analiz etme ve bu tehlikeleri minimize etmek için stratejiler geliştirme sürecidir. Özellikle denizcilik sektöründe, bu süreç, gemilerin güvenliğini sağlamak ve çevresel etkileri azaltmak için kritik öneme sahiptir. MSC.428(98) sayılı karar, siber risk yönetimini güvenlik yönetim sistemlerine entegre etmeyi teşvik etmektedir (Kanwal vd., 2022). Bu tür bir risk yönetiminin uygulanması, hem insan faktörlerini hem de teknolojik unsurları dikkate alarak, işletmelerin siber tehditlere karşı daha dayanıklı hale gelmesini sağlayacaktır.

2.1.3.2 Güvenlik politikaları ve prosedürleri

Kapsamlı güvenlik politikaları ve prosedürleri geliştirmek, bir kuruluşun bilgi güvenliğine yönelik stratejik yaklaşımını belirlemek ve bu yaklaşımı tutarlı bir şekilde uygulamak için hayati öneme sahiptir. Bu belgeler, kuruluşun güvenlik altyapısının temelini oluşturarak, tüm çalışanlar ve paydaşlar için net bir rehberlik sağlar.

Güvenlik politikaları ve prosedürleri, kuruluş içindeki çeşitli rollerin ve sorumlulukların ayrıntılı bir şekilde tanımlanmasını içerir; bu sayede her birey veya departman, bilgi güvenliği kapsamında kendisinden beklenen görevleri ve yükümlülükleri tam olarak anlayabilir. Ayrıca, kabul edilebilir kullanım politikalarının belirlenmesi, çalışanların kurumsal kaynakları ve bilgileri nasıl kullanmaları gerektiğine dair açık yönergeler sunar, bu da olası ihlallerin önlenmesine yardımcı olmaktadır (Alzamil, 2018).

Bu politikalar, sadece günlük operasyonları değil, aynı zamanda güvenlik olayları durumunda izlenecek adımları da kapsar. Olay yanıt prosedürlerinin net bir şekilde tanımlanması, bir güvenlik ihlali veya siber saldırı meydana geldiğinde hızlı ve etkili bir yanıt verilmesini sağlar. Ayrıca, bu prosedürler, olay sonrası yapılacak analiz ve iyileştirme süreçlerini de içermelidir. Güvenlik politikaları ve prosedürleri,

aynı zamanda yasal ve düzenleyici uyumluluk gereksinimlerini de dikkate almalı, bu gereksinimlere uygunluğun sağlanması için gerekli adımları içermelidir.

2.1.3.3 Eğitim ve farkındalık

Çalışan eğitimi ve farkındalık programları, bir kuruluşun bilgi güvenliği stratejisinin temel yapı taşlarından biri olup, güvenlik bilincine sahip bir kurumsal kültür oluşturmak için kritik öneme sahiptir. Bu programlar, çalışanların siber tehditler ve güvenlik riskleri konusunda bilgi sahibi olmasını sağlarken, aynı zamanda onların günlük iş süreçlerinde nasıl daha güvenli davranacaklarını öğrenmelerine de yardımcı olur.

Düzenli ve güncel eğitimlerin sağlanması, çalışanların hassas bilgileri koruma konusunda bilinçlenmelerini ve bu bilgileri yetkisiz erişimden nasıl koruyacaklarını öğrenmelerini sağlar. Ayrıca, bu eğitimler, güvenlik politikalarına ve prosedürlerine uyulmasının önemini vurgular, böylece çalışanlar kuruluşun güvenlik standartlarını ihlal etmeden görevlerini yerine getirebilirler.

Farkındalık programları, çalışanların güvenlik politikalarını anlamalarını ve uygulamalarını sağlarken, aynı zamanda güvenlik ihlallerinin sonuçları hakkında bilinçlenmelerine yardımcı olur. Bu bağlamda, düzenli bilgi güvenliği eğitimleri, işletmelerin güvenlik kültürünü güçlendirmekte ve çalışanların güvenlik konusundaki sorumluluklarını artırmaktadır. Farkındalık programları ayrıca, çalışanların güvenlik olaylarına karşı nasıl tepki vermeleri gerektiği konusunda pratik bilgiler sunar, böylece bir güvenlik ihlali durumunda hızlı ve etkili bir yanıt verilmesi sağlanır (Gündüzalp, 2021).

Bu tür eğitimler, yalnızca belirli bir süreyle sınırlı kalmamalı, sürekli olarak güncellenmeli ve tüm personelin güvenlik konusunda sürekli bir öğrenme sürecinde olmasını sağlamalıdır. Kuruluş içinde güvenlik bilincine sahip bir kültürün inşa edilmesi, sadece teknolojik önlemlere dayanmak yerine, insan faktörünü de güvenlik stratejisinin merkezine yerleştirir, bu da uzun vadede daha sağlam ve dirençli bir güvenlik duruşu oluşturur.

2.1.3.4 Gözlem ve inceleme

BGYS etkinliğini sürdürebilmek ve değişen tehditlere ve kurumsal ihtiyaçlara uyum sağlayabilmek için sistemin sürekli izlenmesi ve düzenli olarak incelenmesi

kritik bir gerekliliktir. Bu süreç, BGYS'nin dinamik ve proaktif bir yapıda olmasını sağlarken, aynı zamanda potansiyel güvenlik zafiyetlerinin erken tespit edilmesine ve gerekli önlemlerin zamanında alınmasına olanak tanır. Sürekli izleme ve değerlendirme faaliyetleri, bilgi güvenliği süreçlerinin etkinliğini ölçmek, performansını değerlendirmek ve iyileştirmeye açık alanları belirlemek amacıyla düzenli olarak gerçekleştirilen denetimleri içerir.

BGYS gözlem ve incelemesi, işletmelerin bilgi güvenliği politikalarının etkinliğini değerlendirmek ve sürekli iyileştirme sağlamak için kritik bir süreçtir. Bu süreç, iç denetimler, dış denetimler ve performans değerlendirmeleri gibi çeşitli yöntemlerle gerçekleştirilir (Baran ve Şener, 2019). Düzenli denetimler, BGYS'nin belirlenen hedeflere ve yasal düzenlemelere uygunluğunu kontrol ederken, aynı zamanda güvenlik politikalarının ve prosedürlerinin gerçek dünyadaki etkinliğini de test eder.

Bu denetimler, iç ve dış kaynaklı tehditlerin tespit edilmesine, mevcut kontrollerin yeterliliğinin değerlendirilmesine ve gerekli iyileştirme fırsatlarının belirlenmesine olanak tanır. Denetim sonuçlarına dayalı olarak yapılan güvenlik değerlendirmeleri, kuruluşun güvenlik risklerine karşı ne kadar hazırlıklı olduğunu ve hangi alanlarda ek önlemler alınması gerektiğini ortaya koyar.

Güvenlik kontrolleri, belirli periyotlarla veya kritik olaylar sonrasında yapılan testler ve incelemeler aracılığıyla güvenlik mekanizmalarının işlevselliğini değerlendirir. Bu kontroller, hem teknolojik altyapının hem de insan faktörüne dayalı süreçlerin güvenliğinin sağlanması için önemlidir. Düzenli olarak yapılan güvenlik kontrolleri, yeni ortaya çıkan tehditlerle başa çıkmak için mevcut sistemlerin yeterliliğini gözden geçirir ve gerektiğinde bu sistemlerde güncellemeler yapılmasını sağlamaktadır. Bu anlamda zafiyet analizi ve sızma testi gibi yaklaşımlar önem arz etmektedir.

Politika ve prosedürlere yönelik güncellemeler ise, değişen iş hedefleri, yeni teknolojiler ve gelişen tehdit manzarası doğrultusunda BGYS'nin sürekli olarak güncellenmesini gerektirir. Güvenlik politikalarının güncel tehditler karşısında etkili olmasını sağlamak amacıyla, bu politikalar düzenli olarak gözden geçirilmeli ve gerektiğinde yeniden yapılandırılmalıdır. Bu güncellemeler, kuruluşun bilgi güvenliği stratejisinin esnek ve adaptif kalmasına yardımcı olur, bu da hem mevcut

güvenlik risklerine karşı etkin bir koruma sağlar hem de gelecekte ortaya çıkabilecek yeni tehditlere karşı hazırlıklı olmayı mümkün kılar.

2.1.3.5 Olay yönetimi

Olay yönetimi sürecinin temel amacı, güvenlik olaylarını en erken aşamada tespit etmek, bu olayların etkilerini analiz etmek ve kuruluşun bilgi güvenliği üzerinde oluşturabileceği olumsuz sonuçları minimize edecek müdahaleleri hızla gerçekleştirmektir. Çalışmalar, bilgi güvenliği olay yönetiminin, işletmelerin siber tehditlere karşı daha hazırlıklı olmalarını sağladığı ve olayların etkili bir şekilde yönetilmesi için gerekli prosedürlerin oluşturulmasının önemine vurgu yapmaktadır (Zarei ve Sadoughi, 2016).

Olay yönetimi sürecinin ilk aşaması, tehditlerin ve güvenlik ihlallerinin etkin bir şekilde tespit edilmesini sağlamak üzere, kapsamlı izleme ve alarm sistemlerinin kurulmasını içerir. Bu sistemler, hem dijital hem de fiziksel güvenlik açıklarını izleyerek, olağandışı faaliyetlerin hızlı bir şekilde fark edilmesine olanak tanır. Erken tespit, güvenlik olaylarının daha ciddi sonuçlar doğurmadan önce kontrol altına alınabilmesi açısından kritik önem taşır.

Bir sonraki adım, tespit edilen güvenlik olaylarının raporlanmasıdır. Bu aşamada, olayların doğru ve eksiksiz bir şekilde belgelenmesi, hangi sistemlerin etkilendiğinin ve olayın boyutunun belirlenmesi, aynı zamanda ilgili tüm paydaşların bilgilendirilmesi gereklidir. Etkili bir raporlama süreci, kuruluşun olayın tam boyutunu anlamasına ve uygun yanıtları koordine etmesine olanak tanır. Bu raporlamalar, gelecekte benzer olayların önlenmesi için gerekli bilgi birikimini sağlamaktadır.

Olay yönetimi sürecinin üçüncü aşaması, olaylara yanıt verilmesidir. Bu aşamada, önceden tanımlanmış prosedürler doğrultusunda olayın kaynağına yönelik müdahaleler gerçekleştirilir ve bu müdahaleler, olayın daha fazla yayılmasını engellemek için hızla uygulanır. Yanıt süreci, genellikle olayın içeriğine göre değişiklik gösterir ve olayın neden olduğu hasarı sınırlamak, etkilenen sistemleri kurtarmak ve normal operasyonları en kısa sürede yeniden başlatmak için çeşitli teknik ve stratejik adımlar içerir. Olay sonrası değerlendirme ve analiz ise, yanıt sürecinin son aşamasını oluşturur ve bu aşama, olaydan öğrenilen derslerin

kaydedilmesini ve işletme bünyesinde uygulanan BGYS'nin gelecekteki güvenlik olaylarına karşı daha dayanıklı hale getirilmesine büyük ölçüde yardımcı olmaktadır.

2.1.3.6 Varlık yönetimi

Varlık yönetimi, bir işletmenin bilgi varlıklarının güvenliğini sağlamak amacıyla, bu varlıkların tanımlanması, envanterinin çıkarılması ve bu varlıklara yönelik risklerin yönetilmesi sürecini kapsar. Bilgi varlıkları, işletme için değer taşıyan her türlü dijital, fiziksel veya entelektüel varlık olabilir. Bu varlıklar, veri tabanları, yazılımlar, donanımlar, belge arşivleri, personel bilgileri ve fikri mülkiyet hakları gibi unsurlardan oluşabilir.

Varlık yönetimi süreci, hangi varlıkların korunması gerektiğini belirlemeyi, bu varlıkların önceliklendirilmesini ve hangi güvenlik önlemlerinin uygulanması gerektiğini değerlendiren bir süreçtir. Bu süreç, bilgi varlıklarına yönelik potansiyel tehditleri ve güvenlik açıklarını tespit edilmesini sağlar ve bu tehditleri minimize etmek için etkili güvenlik politikalarının geliştirilmesine olanak tanır.

BGYS'nin etkili bir şekilde işlemesi için yöneticiler ve çalışanlar arasında işbirliği sağlanması gerekmektedir. Ayrıca, bilgi güvenliği ilkelerinin (gizlilik, bütünlük ve erişilebilirlik) varlık yönetimi süreçlerine entegre edilmesi, bilgi güvenliğinin sağlanmasında önemli bir rol oynamaktadır (Güler ve Furat, 2022).

2.1.3.7 Uyumluluk ve denetim

Uyumluluk ve denetim, bir işletmenin faaliyetlerini yürütürken ulusal ve uluslararası yasa ve yönetmeliklere, sektör standartlarına ve iç politikalara uygun hareket etmesini sağlamaya yarar. Uyumluluk, bir işletmenin özellikle bilgi güvenliği alanında belirlenen yasal düzenlemelere ve standartlara uygunluğunu garanti altına almak amacıyla gerekli adımları atmasıdır.

ISO/IEC 27001, PCI DSS ve GDPR gibi düzenlemeler, işletmelerin bilgi güvenliği süreçlerini ve politikalarını şekillendirirken, rehberlik sağlar. Uyumluluk süreçleri, sadece yasal yükümlülükleri yerine getirmekle kalmaz, aynı zamanda işletmelerin itibarını korur ve müşterilerinin güvenini sağlamlaştırır. Denetim ise uyumluluğun sağlanıp sağlanmadığını ve uygulanan güvenlik politikalarının etkinliğini değerlendirmek için kullanılan bir araçtır.

Denetim, iç ve dış denetimler yoluyla gerçekleştirilebilir ve bir işletmenin mevcut bilgi güvenliği yapısını inceleyerek potansiyel riskleri ve eksiklikleri ortaya çıkarır. Denetim süreci, güvenlik açıklarının tespit edilmesine, uyum eksikliklerinin giderilmesine ve sürekli iyileştirme fırsatlarının belirlenmesine olana tanır. İç ve dış denetimlere ek zafiyet analizi ve sızma testi yapılması da işletmelerin güvenlik pozisyonlarının tespiti açısından önemlidir.

Düzenli denetimler, işletmelerin değişen tehdit ortamlarına karşı daha hazırlıklı olmasını sağlar ve bilgi güvenliği politikalarının etkinliğini sürdürebilmek için proaktif bir yaklaşım geliştirilmesine katkıda bulunur. Bu bağlamda, bilgi güvenliği yönetim sistemlerinin sürekli olarak gözden geçirilmesi ve güncellenmesi, değişen tehditler ve yasal gereklilikler karşısında kritik bir öneme sahiptir (Tunçbilek, 2024).

2.1.3.8 Sürekli iyileştirme

Sürekli iyileştirme, bir işletmenin BGYS süreçlerini sürekli olarak izleyip değerlendirmesi ve bu süreçlerin etkinliğini artırmak için düzenli olarak güncellemeler yapması anlamına gelmektedir. Bu yaklaşım, sadece mevcut sorunları çözmekle kalmaz, aynı zamanda potansiyel riskleri önceden tespit ederek, güvenlik seviyesini sürekli olarak iyileştirmeyi hedefler.

Sürekli iyileştirme, PUKÖ döngüsüne dayanır ve bu döngü, güvenlik süreçlerinin düzenli olarak gözden geçirilip, güncellenmesine olanak tanır. Bu şekilde, değişen tehdit ortamına uyum sağlanabilir ve işletmelerin bilgi güvenliği süreçleri dinamik bir yapı kazanır. Sürekli iyileştirme, işletmenin performansını artırmak ve uyumluluk standartlarını daha yüksek seviyelerde karşılamak için atılan adımları da kapsar.

Bu süreç, teknolojik çözümlerle sınırlı olmayıp, çalışanların denetimi, farkındalık programlarının güncellenmesi ve güvenlik politikalarının düzenli olarak gözden geçirilmesi gibi insan faktörüne dayalı önlemler de içerir (Baran ve Şener, 2019). Sürekli iyileştirme stratejisi, bilgi güvenliğinin işletme içinde yalnızca bir gereklilik değil, aynı zamanda kültürel bir öncelik haline gelmesine yardımcı olur.

2.1.4 ISO 27001'in bilgi güvenliği açısından önemi

Veri ihlallerinin ve siber tehditlerin giderek yaygınlaştığı bir çağda, kuruluşlar bilgi varlıklarının korunmasına öncelik vermelidir. Bunu başarmanın en etkili yollarından biri, ISO/IEC 27001 standardına dayalı bir Bilgi Güvenliği Yönetim Sisteminin uygulanmasıdır. Uluslararası alanda tanınan bu çerçeve, hassas bilgileri yönetmek, gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için yapılandırılmış bir yaklaşım sunmaktadır.

ISO 27001, işletme bünyesinde BGYS kurmak, uygulamak, sürdürmek ve sürekli olarak iyileştirmek için kapsamlı bir çerçeve sunmaktadır. Standart, bilgi varlıklarını çeşitli tehditlerden korumak için gerekli olan risk değerlendirmesi, güvenlik kontrolleri ve sürekli izlemeyi içeren sistematik bir yaklaşımı ana hatlarıyla belirtir. Kuruluşlar, ISO 27001'e uyarak yalnızca mevcut riskleri ele almakla kalmayıp aynı zamanda gelecekteki zorlukları da öngören sağlam bir güvenlik duruşu oluşturabilirler.

ISO 27001, bilgi güvenliğine yönelik risk temelli bir yaklaşımın önemini vurgulamaktadır. İşletmelerin bilgi varlıklarına yönelik potansiyel riskleri belirlemeleri ve bu riskleri azaltmak için uygun kontrolleri uygulamaları gerekmektedir. Bu proaktif yaklaşım, siber saldırıların daha karmaşık ve sık hale geldiği günümüz tehdit ortamında hayati öneme sahiptir (Mirtsch vd., 2021).

ISO 27001'in bir diğer kritik yönü ise, çeşitli yasal ve düzenleyici gerekliliklere uyumu kolaylaştırmadaki rolüdür. ISO 27001'e dayalı bir BGYS'nin uygulanmasının, işletmelerin GDPR gerekliliklerini karşılamalarına önemli ölçüde yardımcı olmaktadır. Gizlilik, bütünlük ve kullanılabilirlik için tüm ilgili kontrollerin yerinde olduğundan emin olarak, işletmeler veri korumasına ve düzenleyici standartlara uyuma olan bağlılıklarını kanıtlayabilmektedir.

İşletmeler, veri koruma uygulamaları konusunda düzenleyiciler ve paydaşlar tarafından giderek daha fazla incelemeye tabi tutuldukça, ISO 27001 sertifikası yüksek güvenlik standartlarını sürdürme konusundaki özverilerinin bir kanıtı olarak hizmet etmektedir. Bu sertifika yalnızca bir kuruluşun güvenilirliğini artırmakla kalmaz, aynı zamanda müşteriler ve ortaklar arasında güven oluşturur ve bu da pazarda rekabet avantajını sürdürmek için olmazsa olmazdır (Rifai, 2023).

ISO 27001 işletmeler için, çalışanların bilgi güvenliği uygulamalarına dahil olmasına teşvik etmekte ve böylece hassas bilgileri korumak için kolektif bir sorumluluk bilinci aşılamaktadır. Eğitim ve farkındalık programları, tüm çalışanların bilgi güvenliğini sürdürmedeki rollerini anlamalarını sağlayarak bir BGYS'nin ayrılmaz bileşenleridir. Güvenlik bilincine sahip bir kültür geliştirerek, işletmeler, güvenlik ihlallerine yol açan insan hatalarının olasılığını önemli ölçüde azaltabilir. İyi bilgilendirilmiş bir iş gücü, potansiyel tehditleri tanımak ve uygun şekilde yanıt vermek için daha disiplinli olduğundan, kuruluşun genel güvenlik duruşunu iyileştirir.

ISO 27001 statik bir çerçeve değildir; bilgi güvenliği uygulamalarında sürekli iyileştirme ihtiyacını vurgular. Standart, kuruluşları değişen tehditlere ve iş ortamlarına uyum sağlamak için ISMS'lerini düzenli olarak gözden geçirmeye ve güncellemeye teşvik eder. Genellikle Planla-Uygula-Kontrol Et-Önlem Al (PUKÖ) döngüsü olarak adlandırılan bu yinelemeli süreç, kuruluşların ortaya çıkan risklere karşı uyanık ve duyarlı kalmasını sağlar (Jevelin, 2023). ISO 27001 çerçevesinin dinamik yapısı, kuruluşların güvenlik önlemlerini sürekli olarak iyileştirmelerine olanak tanır ve ortaya çıktıkça yeni zorluklarla başa çıkabilecek şekilde donatılmalarını sağlar. Bu uyum yeteneği, özellikle hızlı teknolojik gelişmeler ve değişen siber tehditler karşısında büyük önem taşımaktadır.

2.1.5 BGYS risk yönetimi

Bilgi Güvenliği Yönetim Sistemleri, kuruluşların hassas bilgileri korumak ve ilişkili riskleri etkili bir şekilde yönetmek için uyguladığı temel çerçevelerdir. Bir BGYS'nin başarısının merkezinde, bilgi varlıklarına yönelik riskleri belirlemeyi, değerlendirmeyi ve azaltmayı içeren risk yönetimi bileşeni yer alır. Risk yönetimi, bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini tehlikeye atabilecek riskleri belirleme, analiz etme ve bunlara yanıt verme konusunda sistematik bir yaklaşımı ifade etmektedir.

ISO 27001 bir BGYS kurmak için gerekli çerçeveyi sağlarken, ISO 27005 özellikle risk değerlendirme süreçleri de dahil olmak üzere güvenlik risklerini yönetmeye odaklanır. Bu ikili yaklaşım, işletmelerin yalnızca uluslararası standartlara uymasını değil, aynı zamanda risk yönetiminde en iyi uygulamaları benimsemesini de sağlar (Fathurohman ve Witjaksono, 2020).

Risk yönetimi süreci genellikle birkaç temel adımı içerir: risk tanımlama, risk değerlendirmesi, risk tedavisi ve devam eden izleme. Bu adımların her biri, bir kuruluşun karşılaştığı riskleri kapsamlı bir şekilde anlamak ve bu riskleri azaltmak için etkili kontroller uygulamak için çok önemlidir. Risk yönetimi; Risk Tanımlama, Risk Analizi, Risk Değerlendirmesi, Risk İyileştirmesi ve Risk Gözlem/İnceleme olarak dört adımdan oluşmaktadır.

2.1.5.1 Risk tanımlama

BGYS kapsamında risk tanımlama, bilgi varlıklarını korumak için ilk adımdır. Risk tanımlama süreci, potansiyel tehditlerin ve zayıf noktaların belirlenmesini içerir. Bu süreç, bilgi güvenliği risklerinin sistematik bir şekilde değerlendirilmesine olanak tanır ve işletmelerin güvenlik stratejilerini oluşturmasına yardımcı olur. ISO/IEC 27001 standardı, bilgi güvenliği risk yönetim sürecinin temelini oluşturarak, risk tanımlama, analiz etme ve önceliklendirme aşamalarını düzenler (Wibowo ve Ramli, 2022).

Risk tanımlama, bir kuruluşun bilgi varlıklarını korumak için kritik bir süreç olan potansiyel tehditleri ve güvenlik açıklarını tanımayı içerir. Etkili bir risk yönetimi sürecinin temeli, kuruluşun karşı karşıya olduğu çeşitli tehditleri ve bu tehditlerin hangi güvenlik açıklarından yararlanabileceğini anlamaktan geçer. Bu nedenle, kuruluşlar yalnızca mevcut teknolojik sistemlerin zayıflıklarını değil, aynı zamanda çevresel ve insan faktörlerinden kaynaklanabilecek riskleri de dikkate almalıdır. Teknolojik riskler, yazılım ve donanım zafiyetleri, siber saldırılar, veri ihlalleri ve sistem arızaları gibi unsurları kapsar. Bu tür riskler, genellikle hızla gelişen teknolojiyle birlikte değişebilir ve bu nedenle sürekli izleme ve güncellemeler gerektirir.

Çevresel faktörler, doğal afetler, yangınlar, su baskınları veya diğer çevresel olaylar gibi fiziksel tehditleri içerir. Bu tür olaylar, veri merkezleri, sunucular ve diğer kritik altyapılar için önemli tehditler oluşturabilir ve bu nedenle afet kurtarma planlarının geliştirilmesi ve uygulanması kritik öneme sahiptir. Ayrıca, bu faktörler sadece altyapı üzerinde değil, iş sürekliliği üzerinde de ciddi etkilere sahip olabilir, bu yüzden çevresel risklerin yönetimi bütüncül bir yaklaşımla ele alınmalıdır.

İnsan faktörleri ise, iç tehditler, sosyal mühendislik saldırıları, personel hataları ve kasıtlı sabotaj gibi çeşitli riskleri içerir. İnsan hataları, çoğu zaman bilgi

güvenliği açıklarının en yaygın nedenlerinden biri olup, farkındalık eğitimleri ve güvenlik politikaları ile yönetilmesi gereken bir alandır. Ayrıca, çalışanların bilgi güvenliği konusundaki bilinç düzeyini artırmak, iç tehditlere karşı koruma sağlamanın önemli bir bileşenidir.

Risk kaynaklarının tanınması, kuruluşun güvenlik stratejisinin temelini oluşturur ve bu stratejinin etkin bir şekilde uygulanabilmesi için bu faktörlerin tümünün dikkatlice değerlendirilmesi gereklidir. Her bir risk kaynağı, kuruluşun bilgi varlıkları üzerinde farklı seviyelerde tehdit oluşturabilir ve bu nedenle, tüm bu kaynakların bütüncül bir yaklaşımla ele alınması, kapsamlı bir güvenlik politikasının geliştirilmesi ve uygulanması için esastır. Bu adım, kuruluşun bilgi varlıklarını koruma konusunda proaktif bir yaklaşım benimsemesini sağlar ve uzun vadede güvenlik ihlallerinin önlenmesine yardımcı olur.

2.1.5.2 Risk değerlendirmesi

BGYS kapsamında risk değerlendirmesi, bilgi varlıklarını korumak için oldukça önemli bir süreçtir. Risk değerlendirmesi, potansiyel tehditlerin ve zayıf noktaların belirlenmesi, bu tehditlerin olası etkilerinin analiz edilmesi ve risklerin önceliklendirilmesi aşamalarını içerir. Bu süreç, işletmelerin güvenlik stratejilerini oluşturmasına yardımcı olurken, aynı zamanda bilgi güvenliği ihlallerinin önlenmesine yönelik proaktif önlemler almasına olanak tanır (Zarei ve Sadoughi, 2016).

Riskler tanımlandıktan sonra, kuruluşların bu risklerin potansiyel etkilerini ve olasılıklarını dikkatlice değerlendirmesi gerekir. Bu değerlendirme süreci, her bir riskin kuruluş üzerindeki olası sonuçlarını anlamayı ve bu risklerin gerçekleşme olasılıklarını belirlemeyi amaçlar. Risklerin olasılığı ve etkisi, genellikle çeşitli faktörlere dayalı olarak analiz edilir; bunlar arasında riskin doğası, ilgili sistem veya süreçlerin hassasiyeti ve mevcut güvenlik kontrollerinin etkinliği yer alır.

Olasılık ve etki seviyeleri belirlendikten sonra, bu bilgiler kullanılarak riskler ciddiyetlerine göre sınıflandırılır ve önceliklendirilir. Bu sınıflandırma, kuruluşun hangi risklerin acilen ele alınması gerektiğini ve hangi risklerin kabul edilebilir seviyelerde yönetilebileceğini belirlemesine yardımcı olur. Önceliklendirme süreci, kuruluşun risk toleransı, yani hangi seviyede risk kabul edilebilir bulunduğu göz önünde bulundurularak gerçekleştirilir.

Bazı riskler, düşük olasılıklı ancak yüksek etkili olabilirken, diğerleri daha sık karşılaşılabilecek ancak daha az zarar verici olabilir. Bu nedenle, risk değerlendirmesi sırasında, risklerin olası maliyetleri, operasyonel kesintilere neden olma potansiyeli, itibar kaybı gibi unsurların tümü dikkate alınmalıdır. Yüksek öncelikli riskler, kuruluşun hayati varlıklarını tehdit edebilecek, büyük mali kayıplara veya düzenleyici ihlallere yol açabilecek risklerdir ve bu tür risklerin hızlı bir şekilde ele alınması gereklidir.

Etkili bir risk değerlendirmesi, yalnızca risklerin ciddiyetine odaklanmakla kalmaz, aynı zamanda mevcut güvenlik kontrollerinin bu riskleri ne kadar iyi yönettiğini de değerlendirmeyi içerir. Bu değerlendirme, mevcut güvenlik önlemlerinin yeterliliğini analiz eder ve güvenlik açıklarını belirleyerek, hangi alanlarda ek önlemler alınması gerektiğini ortaya koyar.

Mevcut güvenlik kontrolleri, bazı riskleri azaltmada yeterli olabilirken, diğerleri için daha güçlü veya ek tedbirler gerekebilir. Bu süreç, kuruluşun kaynaklarını en verimli şekilde kullanmasını sağlar ve hangi risklerin azaltılması gerektiği ve hangi alanların daha fazla yatırım gerektirdiği belirlenmiş olur.

2.1.5.3 Risk iyileştirmesi

Risk değerlendirmesi, potansiyel tehditlerin ve zayıf noktaların belirlenmesi, bu tehditlerin olası etkilerinin analiz edilmesi ve risklerin önceliklendirilmesi aşamalarını içerir. Yapılan araştırmalar, bilgi güvenliği risk yönetiminin etkin bir şekilde uygulanmasının, işletmelerin bilgi güvenliği stratejilerini güçlendirdiği ve güvenlik ihlallerinin önlenmesine katkıda bulunduğu vurgulanmıştır (Alcántara ve Melgar, 2016). Bu süreç, işletmeler açısından güvenlik stratejilerini oluşturmasına yardımcı olurken, aynı zamanda bilgi güvenliği ihlallerinin önlenmesine yönelik proaktif önlemler almasına olanak tanır.

Riskleri değerlendirdikten sonra, işletmelerin bu riskleri etkili bir şekilde yönetmek ve minimize etmek için uygun önlemler alması gerekmektedir. Bu aşama, risk yönetim sürecinin kritik bir parçasıdır ve kuruluşun bilgi güvenliğini ve operasyonel sürekliliğini koruma çabalarının merkezinde yer alır. Risklerin doğası ve ciddiyetine göre belirlenen iyileştirme önlemleri, kuruluşun karşı karşıya olduğu tehditleri azaltmayı, ortadan kaldırmayı veya kontrol altına almayı hedefler. Bu çerçevede, kuruluşlar çeşitli stratejiler benimseyebilir; bunlar arasında güvenlik

kontrollerinin uygulanması, sigorta yoluyla riski aktarma, riski kabul etme veya transfer etme gibi yaklaşımlar bulunur.

Güvenlik kontrolleri, riskleri doğrudan azaltmaya yönelik en yaygın kullanılan stratejilerden biridir. Bu kontroller, teknik, idari veya fiziksel olabilir ve genellikle riski kabul edilebilir bir seviyeye indirmek için tasarlanır. Teknik kontroller, güvenlik duvarları, antivirüs yazılımları, şifreleme teknikleri ve erişim kontrol mekanizmaları gibi teknolojik çözümleri içerir.

İdari kontroller, politika ve prosedürlerin oluşturulmasını, personelin eğitilmesini ve düzenli denetimlerin yapılmasını kapsar. Fiziksel kontroller ise, veri merkezlerinin güvenliği, kilitli odalar, güvenlik kameraları ve giriş çıkış denetimleri gibi önlemleri içerir. Bu kontroller, tehditlerin gerçekleşme olasılığını azaltarak, kuruluşun risk seviyesini düşürür.

Riskin aktarılması, riski tamamen ortadan kaldırmaktansa, riskin finansal etkilerini yönetmeyi amaçlayan bir stratejidir. Bu yaklaşım, özellikle büyük finansal kayıplara yol açabilecek riskler için geçerlidir. Sigorta poliçeleri, belirli olayların veya ihlallerin gerçekleşmesi durumunda, finansal kayıpları telafi etmek üzere tasarlanmıştır.

Bu durum, kuruluşun büyük bir mali yüke maruz kalmasını engeller ve risklerin yönetimini daha öngörülebilir hale getirir. Ancak, sigorta stratejisi, riski tamamen ortadan kaldırmaz; sadece bu riskin etkilerini hafifletir, dolayısıyla sigorta, genellikle diğer güvenlik önlemleriyle birlikte kullanılır.

Bazı durumlarda, riskler kabul edilebilir seviyelere düşürüldüğünde veya kontrol altına alındığında, kuruluşlar bu riskleri bilinçli olarak kabul edebilir. Bu, özellikle riskin düşük olasılıkla gerçekleşeceği ancak etkisinin sınırlı olacağı durumlarda tercih edilir. Riskin kabul edilmesi, kuruluşun belirli bir düzeyde riskle yaşamayı kabul ettiği anlamına gelir ve bu karar, genellikle maliyet-etkinlik analizleri ile desteklenir. Riskin kabul edilmesi, riskin tamamen ortadan kaldırılmasının veya kontrol altına alınmasının ekonomik olarak mantıklı olmadığı durumlarda makul bir seçenek olabilir.

2.1.5.4 Gözlem ve inceleme

Risk yönetimi, tek seferlik bir faaliyet olarak ele alınamaz; aksine, dinamik ve sürekli bir süreçtir. Bu süreç, işletmelerin sürekli olarak değişen tehditler ve iş ortamlarına uyum sağlayabilmesine yardımcı olmak için düzenli izleme, değerlendirme ve iyileştirme faaliyetlerini içerir. Modern iş dünyasında, risk faktörleri ve tehdit manzarası hızla değişebilir; yeni teknolojilerin benimsenmesi, düzenleyici ortamların evrimi, ve siber tehditlerin giderek daha sofistike hale gelmesi gibi unsurlar, risklerin sürekli olarak yeniden değerlendirilmesini zorunlu kılar. Bu bağlamda, risk yönetimi süreci, kuruluşların hem mevcut hem de ortaya çıkan risklere karşı proaktif bir duruş sergileyebilmesi için sürekli bir gözden geçirme ve uyarlama gerektirir.

İşletmeler, risk manzaralarını düzenli olarak yeniden değerlendirmeli ve ortaya çıkan yeni tehditleri, zafiyetleri ve iş fırsatlarını dikkate alarak Bilgi Güvenliği Yönetim Sistemlerini (BGYS) buna göre güncellemelidir. Bu süreç, hem iç hem de dış kaynaklardan gelen verilerin sürekli analiz edilmesini ve bu veriler ışığında güvenlik politikalarının, prosedürlerinin ve kontrollerinin iyileştirilmesini içerir. Düzenli olarak yapılan risk değerlendirmeleri, yalnızca mevcut güvenlik açıklarının ve kontrollerinin etkinliğini test etmekle kalmaz, aynı zamanda işletmenin iş hedeflerine ve risk toleransına uygun olarak hangi alanlarda ek önlemler alınması gerektiğini de belirler.

Periyodik incelemeler, risk yönetimi sürecinin ayrılmaz bir parçasıdır ve bu incelemeler, BGYS'nin zaman içinde ne kadar etkili olduğunu ve yeni tehditlere karşı nasıl performans gösterdiğini değerlendirmek için kritik öneme sahiptir. Bu incelemeler, ayrıca, önceki risk değerlendirmeleri sonucunda uygulanan iyileştirme önlemlerinin başarısını ve bunların işletmenin genel güvenlik duruşu üzerindeki etkisini ölçmek için de kullanılır.

İnceleme süreçleri, güvenlik açıklarının belirlenmesine, zayıf noktaların düzeltilmesine ve başarılı uygulamaların pekiştirilmesine yardımcı olur. Sürekli izleme ve periyodik değerlendirmeler, risk yönetiminin etkinliğini sürdürmek için zorunludur. Bu süreçler, yalnızca güvenlik açıklarının belirlenmesi ve giderilmesi için değil, aynı zamanda işletmenin değişen iş ortamında esnek ve dirençli kalmasını sağlamak için de gereklidir.

ISO 27001, kuruluşların en iyi uygulamaları takip etmesini ve yasal ve düzenleyici gerekliliklere uymasını sağlayarak risk yönetimine yapılandırılmış bir yaklaşım sağlamaktadır (Ewuga, 2024). Ayrıca, ISO 27001 çerçevesi, bilgi güvenliği yatırımları ve kaynak tahsisi konusunda etkili karar alma için gerekli olan risk tabanlı bir yaklaşımın önemini vurgulamaktadır.

ISO 27005'in BGYS çerçevesine entegre edilmesi, risk yönetimi yeteneklerini daha da güçlendirir. Standart ayrıca, risk değerlendirmeleri yapmak ve güvenlik risklerini yönetmek için ayrıntılı yönergeler sunarak kuruluşların kendi özel ihtiyaçlarını karşılayan özel risk yönetimi stratejileri geliştirmelerine yardımcı olmaktadır. İşletmeler, ilgili standartlara uyarak siber tehditlere karşı dayanıklılıklarını artırabilir ve genel güvenlik duruşlarını iyileştirebilir.

BGYS içinde sağlam risk yönetimi uygulamalarının uygulanması, kuruluşlar için çeşitli faydalar sağlar. Kuruluşlar, riskleri sistematik olarak belirleyip azaltarak güvenlik ihlalleri ve veri kaybı olasılığını önemli ölçüde azaltabilir. Etkili risk yönetimi, kuruluşların çeşitli yasal ve düzenleyici gerekliliklere uymasına yardımcı olur, ceza ve itibar kaybı riskini azaltır.

Risklerin kapsamlı bir şekilde anlaşılması, işletmelerin güvenlik yatırımları ve kaynak tahsisi konusunda bilinçli kararlar almasını ve güvenlik bütçelerini optimize etmesini sağlar. Etkili risk yönetimine bağlılığın gösterilmesi, paydaşların işletmeye ait hassas bilgileri koruma becerisine olan güvenini ve inancını artırır.

2.1.6 BGYS'nin denizcilik sektörü için önemi

Denizcilik sektörü giderek daha fazla dijital teknoloji ve birbirine bağlı sistemleri benimserken, güçlü bilgi güvenliği önlemlerinin önemi de artış göstermektedir. Özellikle ISO/IEC 27001 standardına dayalı bir Bilgi Güvenliği Yönetim Sistemi uygulamak, deniz operasyonlarını siber tehditlere karşı korumak ve denizcilik altyapısının bütünlüğünü sağlamak için önemlidir. Denizcilik sektörü, karmaşık teknolojilere ve birbirine bağlı ağlara olan bağımlılığı nedeniyle benzersiz bir siber güvenlik zorlukları kümesiyle karşı karşıyadır.

Siber saldırılar yalnızca operasyonları aksatmakla kalmamakta, aynı zamanda güvenlik ve emniyet açısından da önemli riskler oluşturmaktadır. Dünya taşımacılığında kritik öneme sahip olan denizcilik sektörü operasyonel bütünlüğü ve güvenliği tehlikeye atabilecek potansiyel tehditlere karşı koruma sağlamak için siber

güvenliğe öncelik vermelidir (Ali vd., 2021). Denizcilik operasyonlarının artan dijitalleşmesi, sektörü siber suçlular ve ulus devlet aktörleri için de çekici bir hedef haline getirmiştir. Navigasyon, iletişim ve kargo operasyonları için gelişmiş teknolojilere güvenilmesi siber olay riskini artırmıştır.

BGYS, bu riskleri yönetmek için yapılandırılmış bir yaklaşım sunarak kuruluşların bilgi varlıklarına yönelik potansiyel tehditleri belirleyebilmesini, değerlendirebilmesini ve azaltabilmesini sağlamaktadır. ISO/IEC 27001 ile uyumlu bir BGYS uygulamak yalnızca güvenliği artırmakla kalmaz, aynı zamanda uluslararası düzenlemelere ve standartlara uyumu da kolaylaştırır. Uluslararası Denizcilik Örgütü (IMO), denizcilik sektöründe siber güvenliği iyileştirmeyi amaçlayan çeşitli yönergeler ve düzenlemeler belirlemiştir.

ISO/IEC 27001'e uyum, paydaşlara bir kuruluşun bilgi güvenliğine öncelik verdiğini ve riskleri yönetmede proaktif olduğunu gösterdiği için rekabet avantajı sağlayabilir. Bu, güven ve güvenilirliğin çok önemli olduğu bir sektörde özellikle önemlidir. ISO/IEC 27001'in uygulanması, denizcilik kuruluşlarının genel dayanıklılığına katkıda bulunur. Risk yönetimi için kapsamlı bir çerçeve oluşturarak, kuruluşlar siber olaylara daha iyi hazırlanabilir ve yanıt verebilir (Kanwal vd., 2022).

Çizelge 2.3: ISO 27001 Kontrolleri ve Denizcilik Operasyonlarına Uygulaması

Kontrol Kategorisi	Açıklama	Denizcilik Operasyonlarına Uygulama
Erişim Kontrolü	Yetkisiz kişilerin sistemlere ve bilgilere erişimini önlemek için kontroller.	Navigasyon sistemlerine, gemi yönetim sistemlerine ve yük izleme yazılımlarına yalnızca yetkili personelin erişimini sağlamak.
Fiziksel Güvenlik	Kritik sistemleri ve altyapıları fiziksel tehditlere karşı koruma.	Gemi veri merkezlerinin, iletişim cihazlarının ve köprü sistemlerinin güvenliğinin sağlanması, sadece yetkili personelin erişimine izin verilmesi.
Olay Yönetimi	Bilgi güvenliği olaylarına müdahale etme ve iyileştirme süreci.	Siber saldırı veya navigasyon sistem arızası gibi olaylara hızlı müdahale edebilmek için olay yönetim süreçlerinin oluşturulması.
İletişim Güvenliği	İletişimlerin güvenliğini sağlamak için tedbirler.	Gemi kaptanı, personel ve karadaki merkezler arasındaki iletişimin güvenliğini sağlamak için şifreleme ve güvenlik protokollerinin uygulanması.
İş Sürekliliği Yönetimi	Kritik operasyonların kesintisiz devamını sağlama.	Deniz operasyonlarında gemi yönetim sistemlerinin çökmesi durumunda alternatif sistemlerin devreye sokulması için iş sürekliliği planlarının hazırlanması.
Tedarikçi İlişkilerinin Yönetimi	Tedarikçilerle güvenlik gereksinimlerini yönetmek	Gemiye donanım veya yazılım sağlayan üçüncü tarafların siber güvenlik standartlarına uymasını sağlamak ve düzenli güvenlik denetimleri yapmak.

Denizcilik sektörü, tüm personelin hassas bilgileri korumadaki rollerini anlamalarını sağlamak için çalışanlar arasında bir siber güvenlik farkındalığı kültürü

geliştirmelidir. Eğitim ve farkındalık programları, çalışanların potansiyel tehditleri tanımasını ve bunlara yanıt vermesini sağlayan güvenlik bilincine sahip bir kültürü teşvik eden bir BGYS'nin ayrılmaz bileşenleridir. Etkili bir BGYS, sürekli iyileştirmeye odaklanmasıyla karakterize edilir.

ISO/IEC 27001 standardı, kuruluşların gelişen tehditlere uyum sağlamasını garanti altına alarak güvenlik önlemlerinde düzenli incelemeler ve güncellemeler yapılması ihtiyacını vurgulamaktadır. Bu yinelemeli süreç, denizcilik işletmelerinin güvenlik uygulamalarını sürekli olarak iyileştirmelerine ve riskleri etkili bir şekilde yönetme yeteneklerini geliştirmelerine olanak tanır. Bilgi güvenliğine risk tabanlı bir yaklaşım benimseyerek, işletmelerin çabalarını karşılaştıkları belirli tehditlere göre önceliklendirebilir, kaynak tahsisini optimize edebilir ve genel güvenlik duruşunu iyileştirebilir (Kitsios vd., 2022).

2.1.7 Nitel risk analizi

Nitel Risk Analizi, risk yönetiminin daha geniş çerçevesinde önemli bir rol oynar ve kuruluşlara yalnızca niceliksel verilere güvenmeden riskleri belirleme, değerlendirme ve kategorize etme araçları sağlar. Risk yönetimi, hedeflere ulaşmayı potansiyel olarak engelleyebilecek riskleri belirlemeyi, değerlendirmeyi ve azaltmayı amaçlayan kurumsal stratejinin kritik bir bileşenidir.

Nitel Risk Analizi, özellikle nicel verilerin kıt olduğu veya hızlı bir değerlendirmenin gerekli olduğu senaryolarda değerli bir yaklaşım olarak ortaya çıkmaktadır. Nitel Risk Analizi, riskleri değerlendirmek için sayısal olmayan yöntemler kullanır ve öznel yargının, uzman görüşünün ve tanımlayıcı analizin önemini vurgulamaktadır.

Küresel iş ortamlarının artan karmaşıklığı, çeşitli risk faktörlerinin öngörülemezliğiyle birleşince, Nitel Risk Analizi'nin önemi artmıştır. İstatistiksel modellere ve sayısal verilere dayanan niceliksel yaklaşımların aksine, Nitel Risk Analizi potansiyel etki, olasılık ve tehdidin doğası gibi riskin nitel yönlerine odaklanır. Bu yaklaşım, risklerin karmaşık, belirsiz veya ölçülmesi zor olduğu durumlarda kullanılmaktadır.

Nitel risk analizi, bazı zorluklarla karşılaşabilir. Özellikle, bu tür analizlerin sonuçları genellikle öznel yorumlara dayandığı için, elde edilen bulguların güvenilirliği ve geçerliliği konusunda endişeler olabilir. Ancak yapılan araştırmalar,

nitel risk analizinin çevresel risk değerlendirmelerinde nasıl kullanıldığına dair bilgiler sunmakta ve bu tür yaklaşımların veri eksikliği durumlarında etkili bir alternatif olabileceğini vurgulamaktadır (Dvořák vd., 2020). Bu nedenle, nitel risk analizi, işletmelerin risk yönetimi süreçlerini güçlendirmek için önemli bir araç olmasına rağmen, dikkatli bir uygulama ve değerlendirme gerektirmektedir.

2.1.7.1 Risk kategorizasyonu

Risk kategorizasyonu, riskleri özelliklerine, potansiyel etkilerine ve meydana gelme olasılıklarına göre sınıflandırmak için kullanılan sistematik bir yaklaşımdır. Bu süreç, kuruluşların riskleri önceliklendirmesini ve bunları azaltmak için kaynakları etkili bir şekilde tahsis etmesini sağlamaktadır (Mochtar ve Rw, 2012). Değerlendirme sürecinin tamamlanmasının ardından, riskler belirlenen etkilerine ve olasılıklarına göre kategorize edilir.

Kategorizasyon süreci, risk yönetimi stratejisinin önemli bir bileşenidir ve risklerin yönetilmesi ve azaltılması için gerekli önceliklerin belirlenmesinde kritik bir rol oynar. Risklerin etkileri ve olasılıklarına göre sınıflandırılması, işletmenin hangi risklere acilen müdahale etmesi gerektiğini ve hangi risklerin daha düşük öncelikli olduğunu netleştirir. Bu sayede, işletmenin sınırlı kaynaklarını en verimli şekilde kullanması ve en kritik riskleri hedef alması sağlanır. Kategorizasyon aynı zamanda risklerin benzer özelliklere sahip gruplar altında toplanmasını mümkün kılar, bu da risk yönetimi sürecini daha sistematik ve yönetilebilir hale getirmektedir.

Risklerin kategorize edilmesi, işletmenin genel stratejik hedeflerine uygun olarak kaynak tahsisinde etkinliği artırır. Operasyonel riskler, günlük iş süreçlerini etkileyebilecek risklerdir ve iş sürekliliği açısından önemlidir. Finansal riskler, işletmenin mali durumunu tehdit edebilecek risklerdir ve bu tür risklerin yönetilmesi, finansal sürdürülebilirliği sağlamak için kritiktir.

Uyumluluk riskleri ise, yasal ve düzenleyici gerekliliklerin ihlal edilmesinden kaynaklanabilecek riskleri içerir ve bu risklerin yönetilmesi, işletme itibarını ve yasal durumunu koruma açısından büyük önem taşır. Bu tür bir kategorizasyon, risk yönetimi sürecinde hangi risklerin daha öncelikli olarak ele alınması gerektiği konusunda netlik kazandırmaktadır.

Kategorizasyon süreci, yalnızca kaynak tahsisini optimize etmekle kalmaz, aynı zamanda paydaşlar arasındaki iletişimi de büyük ölçüde kolaylaştırır. Farklı

paydaş grupları, genellikle farklı risk türlerine odaklanır; bu nedenle, risklerin kategorize edilmesi, tüm tarafların söz konusu riskler hakkında ortak bir anlayış geliştirmesine yardımcı olur. Bu ortak anlayış, risk yönetimi sürecinin daha şeffaf ve katılımcı bir şekilde yürütülmesini sağlamaktadır.

2.1.7.2 Beyin fırtınası

Beyin fırtınası, grup ortamında çok sayıda fikir üretilmesini teşvik eden yaratıcı bir problem çözme tekniğidir. 1950'lerde Alex Osborn tarafından geliştirilen beyin fırtınası, katılımcıların eleştiri korkusu olmadan düşüncelerini ve önerilerini özgürce ifade edebilecekleri açık ve yargılayıcı olmayan bir ortam yaratmayı amaçlar. Süreç genellikle oturumu yönlendiren, katılımcıları birbirlerinin fikirleri üzerine inşa etmeye ve çeşitli bakış açılarını keşfetmeye teşvik eden bir kolaylaştırıcıyı içerir (Gero vd., 2013). Bu yöntem, yenilikçi düşünmeyi teşvik etmek ve karmaşık sorunlara çözümler geliştirmek için tasarım, pazarlama ve proje yönetimi dahil olmak üzere çeşitli alanlarda yaygın olarak kullanılmaktadır.

Beyin fırtınası oturumları, Nitel Risk Analizi'nde yaygın olarak kullanılan ve özellikle yaratıcı düşünme süreçlerini teşvik eden etkili bir risk tanımlama tekniğidir. Bu oturumlar, çeşitli paydaşların bir araya gelerek potansiyel riskleri belirlemek amacıyla serbest ve açık bir şekilde fikirlerini paylaştıkları bir ortam oluşturur. Bu teknik, katılımcıların farklı perspektiflerden bakarak, bir araya geldiklerinde tek başına fark edilemeyebilecek riskleri ortaya çıkarmalarına olanak tanır.

Beyin fırtınası oturumlarının en önemli avantajlarından biri, risklerin belirlenmesi sürecine katılan her bireyin, kendi bilgi ve tecrübelerini ortaya koyarak katkıda bulunmasını teşvik etmesidir. Bu katılımcı yaklaşım, hem daha geniş bir risk yelpazesinin tanımlanmasını sağlar hem de işletme genelinde risk bilincinin artırılmasına yardımcı olur. Bu tür oturumlar, çeşitli paydaşların farklı disiplinlerden gelen uzmanlıklarını ve deneyimlerini bir araya getirdiği için, belirli bir riski daha derinlemesine analiz etmek ve bu riskin potansiyel etkilerini daha iyi anlamak açısından büyük değer taşır.

Beyin fırtınası sırasında ortaya atılan fikirler, katılımcılar tarafından değerlendirildikçe, daha önce gözden kaçmış veya yeterince dikkate alınmamış riskler de gün yüzüne çıkabilir. Bu süreç, yalnızca mevcut risklerin değil, aynı zamanda gelecekte ortaya çıkabilecek olası tehditlerin de öngörülmesini sağlar.

Katılımcıların serbestçe fikir paylaşabilmesi, oturumun daha verimli geçmesini ve daha yaratıcı çözüm yollarının ortaya çıkmasını sağlar.

Beyin fırtınası oturumlarının başarılı olması için, oturumun iyi bir şekilde planlanması ve yapılandırılması gereklidir. Moderatör, oturumu yönlendiren kişi olarak, tüm katılımcıların aktif olarak sürece dahil olmasını ve farklı bakış açılarını paylaşmasını sağlamalıdır. Ayrıca, oturumun belirli bir yapıya sahip olması, konunun dağılıp etkisiz hale gelmesini önlerken, aynı zamanda verimli bir fikir üretme sürecini destekler.

Oturum sırasında notlar alınması ve ortaya çıkan risklerin sistematik bir şekilde kaydedilmesi, sürecin daha sonra analiz edilmesi ve stratejik kararlar alınması aşamalarında kritik rol oynar. Ayrıca, beyin fırtınası oturumları sonucunda belirlenen riskler, daha sonraki aşamalarda detaylı bir şekilde değerlendirilmek üzere önceliklendirilebilir.

2.1.7.3 Delphi tekniği

Delphi Tekniği, bir grup uzmanın belirli bir konu hakkında fikir birliğine varmalarını sağlamak amacıyla geliştirilmiş, yapılandırılmış ve sistematik bir yöntemdir. Bu teknik, özellikle belirsizliklerin yüksek olduğu ve karmaşık sorunların ele alınması gerektiği durumlarda, uzman görüşlerinin dikkatlice toplanması ve analiz edilmesi için son derece etkili bir araçtır. Delphi Tekniği, uzmanlar arasında doğrudan yüz yüze etkileşimi gerektirmez, bu da grup düşüncesi, baskı ve otorite figürlerinden kaynaklanabilecek önyargıların önüne geçer.

Bunun yerine, uzmanlar, anonim olarak geri bildirim sağlar ve bu geri bildirimler doğrultusunda kendi değerlendirmelerini yeniden gözden geçirirler. Bu süreç, birden fazla turda gerçekleştirilir ve her turda uzmanlar, diğer katılımcıların görüşleri ve argümanları hakkında bilgi edinerek kendi değerlendirmelerini iyileştirirler.

Delphi Tekniği'nin en önemli avantajlarından biri, uzmanların anonim olarak görüşlerini bildirebilmesi ve bu sayede sosyal baskıdan veya diğer uzmanların otoritesinden etkilenmeden objektif bir değerlendirme yapabilmeleridir. Bu anonimlik, katılımcıların daha özgürce ve dürüstçe fikirlerini paylaşmalarını teşvik eder, bu da sürecin genel kalitesini artırır. Her tur sonunda, uzmanların verdiği yanıtlar derlenir ve analiz edilerek, bir sonraki tur için geri bildirim olarak sunulur.

Bu şekilde, uzmanlar, kendi değerlendirmelerini diğer katılımcıların görüşleriyle karşılaştırabilir ve bu bilgiler ışığında, daha dengeli ve kapsamlı bir risk analizi yapabilirler. Süreç, genellikle birkaç tur devam eder ve her tur sonunda uzmanlar arasında daha fazla yakınsama gözlemlenir, bu da nihai olarak daha sağlam ve konsensüs odaklı sonuçların elde edilmesini sağlar.

Delphi tekniğinin temel avantajlarından biri, karar alma süreçlerindeki belirsizlik ve muğlaklıklarla başa çıkma becerisidir. Özellikle ampirik verilerin kıt olabileceği veya uzman yargısının önemli olduğu sağlık hizmetleri, teknoloji tahmini ve politika geliştirme gibi alanlarda faydalıdır (Vernon, 2009). Ancak Delphi tekniğinin etkinliği, uzmanların seçimi, sorulan soruların netliği ve yürütülen tur sayısı gibi faktörlerden etkilenebilir

2.1.7.4 Risk matrisleri

Risk matrisleri, bir kuruluşun karşı karşıya olduğu riskleri etkileri ve olasılıklarına göre görsel olarak haritalamak için kullanılan son derece etkili bir araçtır. Bu matrisler, risk yönetimi sürecinin kritik bir parçası olup, risklerin önceliklendirilmesi ve kaynakların etkili bir şekilde tahsis edilmesi açısından büyük fayda sağlar. Risk matrisleri, genellikle iki eksenden oluşur. Biri riskin gerçekleşme olasılığını, diğeri ise riskin potansiyel etkisini temsil eder. Bu eksenlerin kesişiminde yer alan hücreler, belirli bir riskin genel önem derecesini ortaya koyar ve bu sayede kuruluşun hangi risklere acilen müdahale etmesi gerektiğini, hangilerini ise zaman içinde izleyebileceğini belirlemesine yardımcı olur.

Bu matrisler, risklerin yönetimi ve kontrolü açısından önemli avantajlar sunar. Örneğin, yüksek olasılıkla gerçekleşebilecek ancak düşük etkiye sahip bir risk, genellikle daha düşük öncelikli olarak değerlendirilirken, düşük olasılıkla gerçekleşebilecek ancak yüksek etkiye sahip bir risk daha dikkatli bir inceleme gerektirebilir. Bu tür bir sınıflandırma, kuruluşların risklere yönelik stratejilerini daha bilinçli ve veriye dayalı bir şekilde geliştirmesine olanak tanır. Risk matrisleri, ayrıca, karar vericilerin risklerin göreceli önemini daha hızlı ve net bir şekilde anlamalarına yardımcı olur, bu da zamanında ve etkili müdahaleleri mümkün kılar.

Risk matrislerinin basitliği, geniş bir kullanıcı kitlesi tarafından anlaşılabilir ve uygulanabilir olmasını sağlar. Bu araçlar, karmaşık risk değerlendirmelerinin daha erişilebilir hale getirilmesine ve risk yönetimi sürecine daha geniş bir katılım

sağlanmasına yardımcı olur. Hem üst yönetim hem de operasyonel düzeydeki çalışanlar, risk matrislerini kullanarak, kendi sorumluluk alanlarındaki riskleri daha iyi anlayabilir ve bu risklere yönelik uygun önlemleri planlayabilirler. Ayrıca, matrislerin görsel doğası, risk yönetimi toplantılarında ve stratejik planlama oturumlarında etkin bir iletişim aracı olarak da kullanılabilir, böylece tüm paydaşların risk durumunu hızlı bir şekilde kavraması sağlanmış olur.

Risk matrisleri, aynı zamanda, bir kuruluşun risk profilinin zaman içinde nasıl değiştiğini izlemek için de kullanışlıdır. Düzenli olarak güncellenen risk matrisleri, risklerin evrimini ve mevcut stratejilerin etkinliğini gözlemlemeye olanak tanır. Bu dinamik yapı, risk matrislerinin sadece mevcut durumu değil, aynı zamanda gelecekteki olasılıkları ve etkileri de değerlendirmede kullanılabilmesini sağlar.

Yaygın kullanımına rağmen, risk matrislerinin uygulayıcıların farkında olması gereken bazı sınırlamaları vardır. Karmaşık risklerin iki boyutlu bir formata basitleştirilmesi, riskler arasındaki önemli nüansları ve karşılıklı bağımlılıkları göz ardı edebilir. Bu nedenle, risk matrisleri ilk risk değerlendirmeleri ve önceliklendirme için etkili olabilirken, kuruluşların risk manzaralarının kapsamlı bir şekilde anlaşılmasını sağlamak için bunları daha ayrıntılı analizler ve nitel değerlendirmelerle tamamlamaları hayati önem taşımaktadır (Qazi ve Akhtar, 2020). Bu dengeli yaklaşım, risk yönetimi stratejilerinin etkinliğini artırabilir ve genel kurumsal dayanıklılığı iyileştirebilir.

2.1.7.5 SWOT analizi

SWOT analizi, bir kuruluşun stratejik hedeflerini etkileyebilecek hem iç hem de dış faktörleri sistematik bir şekilde belirlemesine yardımcı olan kritik bir stratejik planlama aracıdır. Bu analiz, kuruluşların mevcut durumlarını daha net bir şekilde anlamalarını sağlayarak, gelecekteki stratejik adımlarını bilinçli bir şekilde atmalarına olanak tanır. SWOT analizi, işletmenin içsel güçlü ve zayıf yönlerini değerlendirirken, dış çevredeki fırsatları ve tehditleri de dikkate alır. Bu sayede, kuruluşlar hem içsel kapasitelerini en iyi şekilde nasıl kullanabileceklerini hem de dış çevredeki değişimlere nasıl uyum sağlayabileceklerini planlayabilirler.

Nitel Risk Analizi bağlamında, SWOT analizi, belirli stratejiler veya projelerle ilişkili riskleri değerlendirmek ve yönetmek için etkili bir araç olarak öne çıkar. Örneğin, bir kuruluş yeni bir pazara girmeyi planlıyorsa, SWOT analizi bu

girişimin başarılı olup olmayacağını etkileyebilecek içsel ve dışsal faktörleri ortaya koyabilir. Güçlü yönlerin tanımlanması, kuruluşun hangi alanlarda rekabet avantajına sahip olduğunu anlamasını sağlarken, zayıf yönlerin belirlenmesi, potansiyel risklerin hangi alanlarda yoğunlaşabileceğini gösterir.

Fırsatlar, işletmenin büyüme ve gelişim potansiyelini işaret ederken, tehditler, dış çevreden gelen ve kuruluşun başarısını olumsuz etkileyebilecek unsurları tanımlar. Bu dört boyutun bir arada değerlendirilmesi, kuruluşların daha kapsamlı ve bilinçli risk yönetimi planları geliştirmelerine yardımcı olur. SWOT analizi, risklerin daha stratejik bir perspektiften ele alınmasını sağlar. Güçlü yönler, kuruluşun mevcut risklere karşı dayanıklılığını artırabilirken, zayıf yönler, risklerin kuruluş üzerindeki olumsuz etkisini artırabilir.

SWOT analizinin de bazı sınırlamaları da bulunmaktadır. Yapılan çalışmalar SWOT analizinin genellikle öznel görüşlere dayandığını ve bu durumun karar alma süreçlerini etkileyebileceğini göstermektedir (Helms ve Nixon, 2010). Ayrıca, SWOT analizinin yalnızca mevcut durumu değerlendirmekle kalmayıp, aynı zamanda gelecekteki fırsatları ve tehditleri de göz önünde bulundurması gerektiği vurgulanmaktadır.

2.1.8 Nicel risk analizi

Nicel Risk Değerlendirmesi, riskleri ve potansiyel etkilerini ölçmek için sayısal veriler, istatistiksel yöntemler ve matematiksel modeller kullanmayı içeren risk yönetiminde kritik bir yaklaşımdır. Risk yönetimi, hedeflere ulaşmayı olumsuz etkileyebilecek riskleri belirlemeyi, değerlendirmeyi ve azaltmayı amaçlayan kurumsal stratejide temel bir süreçtir.

Bu bağlamda, Nicel Risk Değerlendirmesi, riskleri anlamak ve yönetmek için sistematik ve veri odaklı bir yaklaşım sağlayan güçlü bir araç olarak ortaya çıkmaktadır. Öznel yargıya ve tanımlayıcı analize dayanan nitel yöntemlerin aksine Nicel Risk Değerlendirmesi, risklerin olasılığını ve etkisini değerlendirmek için sayısal verileri, istatistiksel modelleri ve matematiksel teknikleri kullanmaktadır.

Küresel operasyonların artan karmaşıklığı, büyük veri kümelerinin ve gelişmiş hesaplama araçlarının kullanılabilirliğiyle birlikte, Nicel Risk Analizi'nin önemini ve uygulanabilirliğini önemli ölçüde artırmıştır. Nicel Risk Analizi, olasılık teorisi, istatistik ve karar bilimi ilkelerine dayanmaktadır. Risk olaylarının olasılığını

ve olası sonuçlarını nicelleştirmeyi ve risk yönetimi kararları için daha nesnel bir temel sağlamayı amaçlamaktadır.

2.1.8.1 Olasılık teorisi

Nicel Risk Analizi'nin merkezinde, risklerin matematiksel olarak değerlendirilmesi ve yönetilmesi için temel bir araç olarak kullanılan olasılık teorisi yer almaktadır. Olasılık teorisi, belirli bir risk olayının gerçekleşme olasılığını ve bu olayın potansiyel etkilerini tahmin etmek için istatistiksel yöntemler sunar.

Bu teori, risklerin nicel olarak ifade edilmesine olanak tanıyarak, belirsizliklerin daha somut bir şekilde analiz edilmesini sağlar. Nicel Risk Analizi, çeşitli olasılık dağılımlarını kullanarak, farklı risk olaylarının olasılığını ve bu olayların doğurabileceği sonuçları tahmin etmeye odaklanır. Bu dağılımlar, risk olaylarının sıklığını ve şiddetini modellemek için kritik öneme sahiptir.

Normal, binom ve Poisson dağılımları gibi olasılık dağılımları, genellikle farklı türdeki risklerin oluşumunu modellemek için kullanılır. Normal dağılım, birçok doğal ve ekonomik süreçte karşılaşılan risklerin tahmin edilmesinde yaygın olarak kullanılır. Bu dağılım, bir risk olayının ortalama etrafında nasıl dağıldığını gösterir ve sapmaların ne sıklıkla meydana gelebileceğini tahmin etmeye yardımcı olur. Örneğin, bir yatırım portföyündeki getiri oranlarının normal dağılımını analiz ederek, belirli bir getiri seviyesinin ne kadar olası olduğunu tahmin edebilirsiniz.

Binom dağılımı ise, belirli bir süre boyunca sabit olasılıkla gerçekleşebilecek iki olasılıklı olayları modellemek için kullanılır. Örneğin, bir ürünün üretim sürecinde başarısızlık veya başarı ile sonuçlanabilecek aşamalarını modellemek için binom dağılımı kullanılabilir. Bu dağılım, her bir olayın bağımsız olduğu ve belirli bir sayıda tekrarlandığı durumlar için uygundur, bu da risk analizinin daha spesifik alanlarda uygulanmasına olanak tanır.

Poisson dağılımı, belirli bir zaman dilimi içinde nadir olayların gerçekleşme sıklığını modellemek için kullanılır. Örneğin, bir yıl içinde bir işletmede meydana gelebilecek siber saldırıların sayısını tahmin etmek için Poisson dağılımı kullanılabilir. Bu dağılım, olayların rastgele ve bağımsız olduğu, ancak belirli bir ortalama hızda gerçekleştiği durumlar için uygundur. Poisson dağılımı, özellikle düşük olasılıklı ancak yüksek etkili olayların tahmin edilmesinde önemli bir araçtır, bu da nadir ama ciddi risklerin yönetilmesinde kritik bir rol oynar.

2.1.8.2 İstatistiksel analiz

İstatistiksel analiz, Nicel Risk Analizi'nde merkezi bir rol oynar ve risklerin derinlemesine incelenmesini, değerlendirilmesini ve yönetilmesini sağlar. Risk parametrelerinin tahmin edilmesi için kullanılan istatistiksel ölçüler arasında ortalama, varyans ve standart sapma yer alır. Ortalama, bir risk olayının beklenen değerini temsil eder ve riskin genel eğilimi hakkında bilgi verir.

Varyans, risk olaylarının bu ortalamadan ne kadar sapabileceğini ölçer ve bu sapmaların büyüklüğü hakkında fikir verir. Standart sapma ise, varyansın karekökü olarak hesaplanır ve riskin yayılma derecesini daha anlaşılır bir şekilde ifade eder. Bu ölçüler, risklerin doğasını anlamak ve potansiyel belirsizlikleri daha iyi yönetmek için kritik öneme sahiptir.

Bunun yanı sıra, istatistiksel analizde kullanılan gelişmiş teknikler, risk verilerinin daha karmaşık bir şekilde incelenmesini sağlar. Regresyon analizi, bir veya daha fazla bağımsız değişkenin risk üzerindeki etkisini belirlemek için kullanılır. Bu teknik, risk faktörleri ile sonuçları arasındaki ilişkiyi modelleyerek, hangi faktörlerin riski artırdığını veya azalttığını anlamaya yardımcı olur.

Monte Carlo simülasyonları, risk analizi sürecinde belirsizlikleri modellemek ve potansiyel sonuçların dağılımını tahmin etmek için yaygın olarak kullanılan bir başka önemli tekniktir. Bu simülasyonlar, bir risk olayının farklı olasılıklar altında nasıl sonuçlanabileceğini belirlemek için binlerce hatta milyonlarca senaryoyu simüle eder.

Bu süreç, belirsizliklerin çeşitli kombinasyonlarının etkilerini değerlendirmeye ve risklerin olası sonuçlarını tahmin etmeye olanak tanır. Monte Carlo simülasyonları, özellikle karmaşık ve çok değişkenli sistemlerde risklerin nasıl şekilleneceğini anlamak için güçlü bir araçtır ve bu da stratejik kararların daha bilinçli bir şekilde alınmasını sağlar.

Bayes çıkarımı ise, yeni verilerin ışığında risk olasılıklarını güncellemeye ve daha hassas tahminlerde bulunmaya yardımcı olan bir tekniktir. Bayes çıkarımı, bir risk olayının olasılığını belirlemek için önceden bilinen bilgileri ve mevcut verileri birleştirir. Bu teknik, özellikle belirsiz ve dinamik ortamlarda, risklerin daha doğru bir şekilde tahmin edilmesi için son derece değerlidir.

2.1.8.3 Karar bilimi

Nicel Risk Analizi, yalnızca risklerin olasılıklarını ve potansiyel etkilerini ölçmekle kalmaz, aynı zamanda bu risklerin yönetiminde kullanılan karar modellerini geliştirmek için karar biliminden de önemli ölçüde yararlanır. Karar bilimi, özellikle karmaşık ve belirsizliklerle dolu ortamlarda stratejik kararların alınmasında kritik bir rol oynar. Bu bilim dalı, karar vericilerin farklı senaryoları sistematik bir şekilde değerlendirmesine olanak tanıyan matematiksel ve analitik araçlar sunar.

Karar modelleri, karar vericilere, karşı karşıya kaldıkları çeşitli risk senaryolarını analiz etme, bu senaryoların muhtemel sonuçlarını değerlendirme ve hangi stratejilerin en etkili olacağını belirleme konusunda yardımcı olur. Bu modeller, genellikle risk azaltma stratejilerinin maliyetlerini ve faydalarını karşılaştırarak, en uygun ve sürdürülebilir çözümleri bulmayı amaçlar. Bu bağlamda, karar modelleri, bir işletmenin risk yönetimi sürecini optimize etmeye yönelik önemli araçlar sağlar. Örneğin, karar ağaçları, olası sonuçları ve bu sonuçların olasılıklarını görselleştirerek, karar vericilerin alternatif stratejileri değerlendirmesine yardımcı olur.

Bu teknik, farklı risk azaltma stratejilerinin potansiyel maliyetlerini ve faydalarını karşılaştırarak, işletme kaynaklarını en etkili şekilde nasıl kullanabileceğini belirlemesine olanak tanır. Benzer şekilde, fayda-maliyet analizi, belirli bir risk yönetimi stratejisinin finansal ve operasyonel etkilerini değerlendirerek, hangi stratejinin en yüksek getiri sağlayacağını gösterir. Bu analiz, özellikle risk yönetimi stratejilerinin ekonomik açıdan uygulanabilirliğini ve sürdürülebilirliğini değerlendirmede son derece önemlidir.

Nicel Risk Analizi'nde kullanılan bu tür karar modelleri, belirsizlik altında daha bilinçli ve veriye dayalı seçimler yapılmasını sağlar. Karar modelleri, yalnızca mevcut risklerin değerlendirilmesine yardımcı olmakla kalmaz, aynı zamanda gelecekte ortaya çıkabilecek potansiyel risklerin de önceden tahmin edilmesine olanak tanır. Bu imkan, işletmeler için daha proaktif ve stratejik bir risk yönetimi yaklaşımının benimsenmesini sağlar.

Karar vericiler, bu modelleri kullanarak, farklı senaryoları simüle edebilir, çeşitli risk azaltma stratejilerini test edebilir ve en uygun stratejileri seçebilir. Bu

süreç, işletmelerin risklere karşı daha esnek ve hazırlıklı olmasını sağlar, bu da uzun vadede iş sürekliliğini ve başarıyı destekler.

2.1.8.4 Hata ağacı analizi (FTA)

Hata Ağacı Analizi (Fault Tree Analysis), karmaşık sistemlerin başarısız olabileceği yolları modellemek ve bu başarısızlıkların kökenine inmek için kullanılan, yukarıdan aşağıya, tümdengelimli bir yaklaşımdır. Bu analitik yöntem, sistemde meydana gelebilecek bir arızanın veya hatanın potansiyel nedenlerini belirlemeye ve bu nedenlerin olasılıklarını nicel olarak değerlendirmeye odaklanır.

FTA, bir sistemdeki olası hataların veya arızaların hiyerarşik bir şekilde ayrıntılandırıldığı bir hata ağacı oluşturur. Bu ağaç, en tepedeki genel sistem arızasıyla başlar ve alt seviyelerde bu arızaya katkıda bulunan tüm alt sistemler ve bileşenler incelenir. Hata Ağacı Analizi'nin amacı, bu alt nedenlerin her birinin genel sisteme olan katkısını analiz ederek, sistem arızasının olasılığını tahmin etmektir.

FTA, hataların temel nedenlerini belirleme sürecinde tümdengelimli bir yaklaşım kullanır; yani, genel bir sistem arızası ya da istenmeyen bir olaydan başlayarak, bu arızaya yol açabilecek tüm potansiyel faktörler ve nedenler aşama aşama analiz edilir. Bu süreç, sistemin hangi bileşenlerinin veya süreçlerinin en kırılgan olduğunu belirlemeye ve bu zayıf noktaların nasıl giderilebileceğine dair stratejiler geliştirmeye yardımcı olur.

FTA, bu tür kök neden analizlerinin sonucunda, sistemin genel güvenilirliğini artırmak ve arıza olasılığını azaltmak için önleyici tedbirlerin alınmasını sağlar. Olasılık hesaplamaları, hatanın temel nedenlerinin her birinin katkısını değerlendirerek, sistemin genel başarısızlık olasılığını tahmin eder. Bu nicel veriler, karar vericilerin hangi alanlara odaklanmaları gerektiğini ve hangi iyileştirme önlemlerinin en etkili olacağını belirlemelerine olanak tanır.

Hata Ağacı Analizi, özellikle güvenilirliğin kritik öneme sahip olduğu endüstrilerde yaygın olarak kullanılır. Havacılık, nükleer enerji, savunma, otomotiv ve yüksek güvenlik gerektiren üretim süreçleri gibi sektörlerde, FTA, sistem güvenilirliğini sağlamada hayati bir araç olarak kabul edilir. Örneğin, bir uçak motorunun güvenilirliği, yolcu güvenliği açısından son derece kritiktir ve FTA, motorun hangi bileşenlerinin arıza yapabileceğini ve bu arızaların uçak için nasıl bir risk oluşturabileceğini modellemek için kullanılabilir.

Benzer şekilde, nükleer enerji santrallerinde, reaktör güvenliği üzerinde çalışan mühendisler, potansiyel arıza modlarını ve bu modların nasıl bir zincirleme reaksiyona yol açabileceğini anlamak için FTA'dan faydalanır. Bu tür analizler, potansiyel tehlikeleri önceden belirleyerek, ciddi kazaları ve felaketleri önlemek için gerekli adımların atılmasını sağlar.

FTA'nın gücü, sistem arızalarının anlaşılmasına ve yönetilmesine katkıda bulunan detaylı ve sistematik bir yapı sunmasından gelir. Hata ağacı, karmaşık sistemlerin daha küçük, yönetilebilir parçalara ayrılmasına yardımcı olur, bu da mühendislerin ve analistlerin her bir bileşenin risk katkısını daha iyi anlamalarına olanak tanır. Ayrıca, FTA sadece mevcut sistemlerin güvenilirliğini değerlendirmekle kalmaz, aynı zamanda yeni sistemlerin tasarımında da proaktif olarak kullanılabilir. Sistem tasarımı sırasında FTA kullanılarak, potansiyel arıza modları önceden tespit edilebilir ve bu arızaların olasılıklarını azaltmak için tasarım iyileştirmeleri yapılabilir.

2.1.8.5 Olay ağacı analizi (ETA)

Olay Ağacı Analizi (Event Tree Analysis), bir sistemde veya süreçte başlatıcı bir olaydan kaynaklanabilecek tüm olası sonuçları modellemek amacıyla kullanılan tümevarımsal, ileriye dönük bir risk analizi yöntemidir. Bu analiz, bir sistemde meydana gelebilecek başlangıç olaylarının farklı sonuçlara nasıl yol açabileceğini adım adım izler ve bu sonuçların her birinin olasılığını hesaplar.

ETA, sistemdeki her bir olayın potansiyel sonuçlarını bir ağaç yapısı şeklinde görselleştirir, bu sayede karar vericiler, bir olayın farklı koşullar altında nasıl gelişebileceğini ve nihai olarak ne tür sonuçlara yol açabileceğini anlayabilir. Bu yöntem, belirli bir olayın doğurabileceği farklı senaryoların ayrıntılı bir analizini sunarak, risk yönetimi ve güvenlik planlaması süreçlerinde kritik bir rol oynar.

Olay Ağacı Analizi'nin temelinde, başlatıcı bir olayın ardından meydana gelebilecek olası olayların sıralı bir şekilde incelenmesi yatmaktadır. ETA, bu tür olaylar zincirinin her adımında, alternatif sonuçların ortaya çıkabileceği noktaları belirler ve bu alternatiflere belirli olasılıklar atar. Her dalın ucunda, olayın gerçekleşme olasılığı ve bunun sonucunda ortaya çıkabilecek potansiyel sonuçlar nicel olarak değerlendirilir. Bu sayede, Olay Ağacı Analizi, bir başlatıcı olayın

sistem üzerinde ne tür etkilere yol açabileceğini ve bu etkilerin olasılıklarını ayrıntılı bir şekilde tahmin eder.

Olay Ağacı Analizi, başlatıcı bir olayla başlayan ve olası sonraki olayların sırasını modelleyen tümevarımsal, ileriye dönük bir yaklaşımdır. Olay ağacının her bir dalına olasılıklar atayarak, ETA farklı sonuçların olasılığının nicel bir tahminini sağlar. Bu yöntem, özellikle kimyasal işleme ve nükleer enerji gibi endüstrilerde güvenlik analizinde yaygın olarak kullanılır.

ETA'nın en büyük avantajlarından biri, olayların ve sonuçlarının sistematik bir şekilde analiz edilmesine olanak tanımasıdır. Olay ağacının her bir dalına olasılıklar atanarak, analiz edilen sistemdeki çeşitli risklerin nicel bir tahmini yapılabilir. Bu süreç, sistemin hangi bölümlerinin en yüksek risk altında olduğunu ve hangi kontrol önlemlerinin bu riskleri azaltmada etkili olabileceğini belirlemekte kritik rol oynar.

Olasılıkların hesaplanması ve olayların birbirine bağlı olarak nasıl geliştiğinin anlaşılması, karar vericilerin risk azaltma stratejilerini optimize etmelerine olanak tanır. ETA ayrıca, farklı güvenlik önlemlerinin veya müdahale stratejilerinin etkinliğini değerlendirmeye ve bu stratejilerin uygulanmasının hangi sonuçları getireceğini öngörmeye de yardımcı olur.

Avantajlarına rağmen, Olay Ağacı Analizi'nin de çeşitli zorlukları bulunmaktadır. Ağacın her bir dalı için doğru olasılık tahminlerine güvenilmesi, önemli bir sınırlama olarak görülmektedir. Bu sınırlama, özellikle birbirine bağımlılıkları olan karmaşık sistemlerde elde edilmesi zor olabilir (Mareş ve Stelea, 2017).

İş kazaları gibi gerçek dünya senaryolarında ETA'nın uygulanması, söz konusu bağlamın ve olası belirsizliklerin dikkatli bir şekilde değerlendirilmesini gerektirir. Bu nedenle, ETA risk değerlendirmesi için değerli bir araç olsa da söz konusu risklerin kapsamlı bir şekilde anlaşılmasını sağlamak için diğer analitik yöntemlerle tamamlanmalıdır.

2.1.8.6 Risk altındaki değer (VaR)

Risk Altındaki Değer (Value at Risk), finansal risk yönetiminde yaygın olarak kullanılan bir ölçüm aracıdır. VaR, belirli bir zaman diliminde ve belirli bir

güven düzeyinde, bir yatırım portföyünün karşılaşabileceği maksimum kaybı tahmin eder. Bu ölçüm, finansal kurumlar ve yatırımcılar için riskin değerlendirilmesi ve yönetilmesi açısından kritik bir öneme sahiptir (Pelletier ve Wei, 2015).

VaR, genellikle bir portföyün riskini belirlemek için kullanılırken, aynı zamanda piyasa riskinin düzenlenmesi ve yönetilmesi için de önemli bir araç olarak kullanılmaktadır. VaR hesaplama yöntemleri arasında tarihsel simülasyon, varyans-kovaryans ve Monte Carlo simülasyonu gibi teknikler bulunmaktadır. Bu yöntemler, farklı varsayımlar ve veri setleri kullanarak VaR değerini hesaplar.

VaR'ın sağladığı avantajlar arasında, basit ve anlaşılır bir risk ölçümü sunması yer alır. Bu durum, hem uzmanlar hem de yatırımcılar için VaR'ın kolaylıkla yorumlanabilmesini sağlar (Krause, 2003). Ancak, VaR'ın bazı sınırlamaları da bulunmaktadır. Örneğin VaR, sadece belirli bir güven düzeyinde maksimum kaybı tahmin edebilmekteyken, kayıpların olasılık dağılımının uç noktalarını göz ardı edebilmektedir. Bu nedenle, VaR'ın yanı sıra, koşullu değer kaybı gibi ek risk ölçümleri de kullanılmaktadır.

VaR'ın finansal piyasalardaki uygulamaları oldukça geniştir. Özellikle portföy optimizasyonu, risk yönetimi ve sermaye gereksinimlerinin belirlenmesi gibi alanlarda yaygın kullanılmaktadır. Ayrıca, Basel düzenlemeleri gibi yasal çerçeveler, finansal kurumları piyasa risklerini yönetmek için VaR kullanımını bir standart olarak kabul etmiştir. Bu bağlamda, VaR'ın etkin bir şekilde kullanılması, finansal istikrarın sağlanması ve risklerin minimize edilmesi açısından kritik bir rol oynamaktadır.

2.1.8.7 Monte Carlo simülasyonu

Monte Carlo simülasyonu, Nicel Risk Analizi'nde özellikle birçok belirsiz değişkene sahip karmaşık sistemleri modellemek için yaygın olarak kullanılan ve son derece güçlü bir tekniktir. Bu yöntem, risklerin karmaşıklığını ve belirsizliklerini anlamak ve yönetmek için matematiksel ve istatistiksel yaklaşımları birleştirir. Monte Carlo simülasyonu, bir risk olayının farklı koşullar altında nasıl sonuçlanabileceğini tahmin etmek için binlerce, hatta milyonlarca simülasyon çalıştırmayı içerir.

Her bir simülasyon, belirli bir dizi girdi değişkenine dayalı olarak farklı sonuçlar üretir ve bu sonuçlar, olası risklerin geniş bir yelpazede değerlendirilmesine

olanak tanır. Bu süreç, risklerin olasılık dağılımlarını ve bu dağılımların potansiyel etkilerini anlamak için detaylı bir analiz sağlar. Monte Carlo simülasyonunun en büyük avantajlarından biri, belirsizliklerin ve değişkenliklerin etkilerini daha iyi anlayarak, farklı senaryoların olasılıklarını ve potansiyel sonuçlarını görselleştirmeye olanak tanımasıdır. Bu yöntem, özellikle belirsizliklerin yüksek olduğu ve risk faktörlerinin çok çeşitli olduğu durumlarda son derece etkilidir.

Örneğin, bir yatırım portföyünün gelecekteki performansını tahmin etmek veya bir projenin tamamlanma süresini ve maliyetini öngörmek için Monte Carlo simülasyonu kullanılabilir. Bu simülasyonlar, farklı olasılık dağılımlarını ve değişkenlerin birbirleriyle olan ilişkilerini dikkate alarak, risklerin en olası sonuçlarını tahmin etmede büyük bir doğruluk sağlar.

Simülasyonlar sonucunda elde edilen veriler, olası risklerin aralığını ve farklı sonuçların olasılığını detaylı bir şekilde analiz etmeyi mümkün kılar. Bu analiz, karar vericilere, hangi risklerin daha büyük bir tehdit oluşturduğunu ve hangi stratejilerin bu riskleri en aza indirebileceğini belirlemede kritik bilgiler sunar. Bu bilgi, karar vericilerin bu riskle ilgili önleyici tedbirler almasını veya sigorta gibi risk azaltma stratejilerini uygulamasını teşvik edebilir.

Monte Carlo simülasyonu ayrıca, hassasiyet analizi için de kullanılabilir. Hassasiyet analizi, hangi değişkenlerin sonuca en fazla etki ettiğini belirlemeye yardımcı olur. Bu durum, işletmelerin hangi faktörlere daha fazla odaklanmaları gerektiğini ve hangi değişkenlerin daha dikkatli izlenmesi gerektiğini anlamalarına olanak tanır.

2.1.9 Risk değerlendirmesi karar süreci

Nitel Risk Değerlendirmesi ile Nicel Risk Değerlendirmesi arasında karar verirken, riskin niteliği ve değerlendirmenin yürütüldüğü bağlam önemli faktörlerdir. Niteliksel yöntemler, risklerin karmaşık, iyi anlaşılmamış veya verilerin kıt veya kolayca ölçülebilir olmadığı durumlar için en uygunudur. Nicel Risk Değerlendirmesi yeterli veri mevcut olduğunda ve risk etkisi ve olasılığının kesin, sayısal tahminlerine ihtiyaç duyulduğunda idealdir. Nicel yöntemler genellikle finans, mühendislik ve çevre yönetimi gibi sektörlerde kullanılır; burada istatistiksel modeller ve Monte Carlo simülasyonları veya Risk Değeri (VaR) gibi olasılıksal teknikler karar alma için sağlam bir temel sağlamaktadır.

Nitel ve nicel yaklaşımlar arasındaki seçim, ilgili paydaşlara ve almaları gereken kararlara da bağlıdır. Paydaşlar stratejik kararları bilgilendirmek için hızlı ve üst düzey bir risk genel görünümüne ihtiyaç duyuyorsa, basitliği ve iletişim kolaylığı nedeniyle nitel bir değerlendirme daha uygun olabilir. Bir diğer husus, daha kapsamlı bir risk değerlendirmesi sunabilen nitel ve nicel yöntemlerin her ikisinin de entegrasyonudur.

Uygulamada, birçok kuruluş başlangıçta riskleri belirlemek ve kategorize etmek için nitel bir yaklaşım kullanır, ardından en kritik risklerin nicel bir analizi yapılır. Bu hibrit yaklaşım, her iki yöntemin güçlü yönlerinden yararlanarak riskler hakkında geniş bir anlayış sağlarken gerektiğinde ayrıntılı, veriye dayalı içgörüler de sunmaktadır.

Çizelge 2.4: Nitel ve Nicel Risk Analizi Arasındaki Temel Farklar

Özellik	Nitel Risk Analizi	Nicel Risk Analizi
Veri Gereksinimleri	Veri kıtlığı durumunda kullanılabilir; subjektif değerlendirmelere dayanır.	Yeterli ve güvenilir veriye ihtiyaç duyar; sayısal analizlerle desteklenir.
Analiz Yaklaşımı	Kalitatif olarak risk seviyelerini sınıflandırma (düşük, orta, yüksek).	Risklerin olasılık ve etkisinin kesin, sayısal tahminlerle ölçülmesi.
Karmaşıklık	Basit ve hızlı; daha az kaynak gerektirir.	Daha karmaşık; istatistiksel ve olasılıksal modellere dayanır.
Kullanım Alanları	Risklerin iyi anlaşılmadığı veya verinin sınırlı olduğu durumlarda uygundur.	Finans, mühendislik gibi verinin bol olduğu ve kesin tahminlerin gerektiği alanlarda kullanılır.
Paydaş Tercihleri	Stratejik kararlar için hızlı, üst düzey bir genel görünüm sağlar.	Sayısal sonuçlar ve kesin risk analizleri gerektiren karar alma süreçlerinde tercih edilir.
Sonuçların Kesinliği	Genellikle subjektif ve göreceli dir; daha genel bir risk profili sunar.	Kesin, objektif ve ölçülebilir sonuçlar sağlar; yüksek doğruluk içerir.
Avantajlar	Kolay uygulanır, hızlı sonuç verir, daha az kaynak gerektirir.	Detaylı, kesin ve sayısal analiz sağlar, risk yönetimi için daha sağlam bir temel sunar.
Dezavantajlar	Subjektif olabilir; kesin sayısal sonuçlar sunmaz.	Zaman alıcı ve kaynak yoğun olabilir; büyük miktarda veri gerektirir.

Nitel veya nicel bir risk değerlendirme yöntemi kullanma kararı, risk değerlendirmesinin özel bağlamı, verilerin kullanılabilirliği, değerlendiricilerin uzmanlığı ve paydaşların ihtiyaçları tarafından yönlendirilmelidir. Bu faktörleri dikkatlice göz önünde bulundurarak, kuruluşlar risklerin etkili bir şekilde tanımlanmasını, değerlendirilmesini ve yönetilmesini sağlamak için en uygun yöntemi veya yöntem kombinasyonunu seçebilir, bu da daha iyi bilgilendirilmiş karar alma ve iyileştirilmiş sonuçlara yol açabilir.

2.2 Siber Güvenlik

Siber güvenlik, bilgisayar bilimi, bilgi sistemleri güvenliği ve teknolojinin çeşitli yönlerini kapsayan çok disiplinli bir alandır. Bilgisayar sistemlerini, ağlarını ve verileri yetkisiz erişime, kullanıma, ifşa edilmeye, kesintiye, değiştirilmeye veya yok edilmeye karşı korumayı içerir. Son yıllarda teknolojiye olan bağımlılığın artması ve siber tehditlerin artması nedeniyle siber güvenliğin önemi önemli ölçüde artmıştır (Samtani vd., 2020).

Siber güvenliğin bir yönü, veri ve iletişimin güvenliğini sağlamak için algoritmaların ve protokollerin kullanımını içeren kriptografidir. Kriptografi, bilgisayar sistemleri ve ağlarındaki bilgilerin gizliliğinin, bütünlüğünün ve gerçekliğinin sağlanmasında çok önemli bir rol oynamaktadır (Zajac, 1994). Siber güvenliğin bir diğer önemli yönü, işletmelerdeki bireylerin davranışlarıdır. Bu nedenle kuruluşların güvenli siber güvenlik davranışları sergilemeleri için çalışanların güvenlik farkındalığını ve yeteneklerini artırmaları gerekmektedir (Anwar vd., 2017).

Ayrıca işletmelerin BT sistemlerinde yer alan cihazlarda koşan işletim sistemleri, servisler, araçlar, yazılımlar ve firmware'lerde bulunan zafiyetler ve bunların hızlı bir şekilde kapatılamaması da büyük bir güvenlik riski oluşturmaktadır. Siber güvenlik açısından önem teşkil eden bir diğer konu da sistemde yer alan cihazların doğru şekilde sıkılaştırılmaması ve gerekli konfigürasyon ayarlarının yapılmamasıdır.

Nesnelerin İnterneti (IoT), siber güvenliğin son derece önem taşıdığı bir diğer alandır. Bağlantılı cihaz sayısının artmasıyla birlikte siber güvenlik riskleri de arttı. Siber güvenlik sertifikasyonu, IoT'deki siber güvenlik risklerini azaltmak için temel bir yaklaşım olarak ivme kazanıyor (Matheu vd., 2020).

Genel olarak siber güvenlik, multidisipliner bir yaklaşım gerektiren karmaşık ve gelişen bir alandır. Kriptografiyi, çalışan davranışlarını, alana özgü hususları, sertifikasyonu ve yapay zeka gibi yeni ortaya çıkan teknolojilerin entegrasyonunu içerir. İşletmelerin bu karmaşık ve grift hususları ele alarak siber güvenlik uygulamalarını geliştirebilir ve siber tehditlere karşı gelişmiş koruma sağlaması gerekmektedir.

2.2.1 Kritik altyapı güvenliği

Kritik altyapı güvenliği, temel sistemleri ve hizmetleri siber tehditlerden korumanın önemli bir yönüdür. Kritik altyapıların korunması hayati öneme sahiptir. Bu sistemlere yapılacak bir saldırı, bir ülkenin ekonomisi, ulusal savunması ve kamu güvenliği açısından ciddi sonuçlar doğurabilir. Kritik ulusal altyapıya yönelik siber tehditlerin ele alınması istihbarat odaklı bir yaklaşım gerektirir. (Rudner, 2013).

Kritik altyapılarda siber güvenliği etkili bir şekilde yönetmek için işletmelerin saldırıların sınıflandırmasını, saldırı vektörlerini ve bu sistemleri hedeflemek için kullanılan saldırı yöntemlerini anlaması gerekir. İşletmelerin güvenlik duruşlarını iyileştirmeye çalışırken yaptıkları yaygın siber güvenlik hatalarını belirlemek de önemlidir (Limba vd., 2017).

Kritik altyapı güvenliğini sağlayabilmek için saldırı vektörlerinin, yaygın hataların ve siber güvenlik faaliyetlerinin acil olarak iyileştirilmesi ihtiyacının kapsamlı bir şekilde anlaşılmasını gerektirir. Ek olarak, denizcilik gibi kritik altyapılara sahip sektörler, kendilerine özgü siber güvenlik sorunlarına çözüm bulmak için özel yaklaşımlar gerektirir. İşletmeler, koruyucu siber güvenlik önlemleri uygulayarak ve istihbarat odaklı bir yaklaşımı benimseyerek riskleri azaltabilir ve kritik altyapıyı siber tehditlerden koruyabilir.

2.2.3 Ağ güvenliği

Ağ güvenliği, bir bilgisayar ağındaki veri ve kaynakların gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamanın önemli bir yönüdür. Ağ altyapısını, cihazları ve verileri yetkisiz erişimden, saldırılardan ve güvenlik açıklarından korumak için önlemlerin uygulanmasını içerir. Ağ güvenliği yerel ağ ve kablosuz ağ olmak üzere ikiye ayrılabilir. Yerel ağ güvenliği daha çok zafiyet analizi ve ağ sıkılaştırması gibi konuları kapsamaktayken, kablosuz ağ daha güvenliği trafiğinin incelenmesine ve potansiyel güvenlik sorunlarının veya anormalliklerinin tanımlanması olarak ifade edilmektedir (Sanders, 2011).

Ağ güvenliği aynı zamanda sosyal medyanın yaygınlaşması, eğitim düzeyi ve siber güvenlik koruma mekanizmaları gibi faktörlerden de etkilenmektedir (Ahangama, 2023). Bu faktörler ile ağ güvenliği arasındaki ilişkiyi anlamak, siber güvenlik uygulamalarını geliştirmeye ve ağları potansiyel tehditlerden korumaya yönelik etkili stratejiler hakkında fikir verebilir.

Ağ güvenliğinin sağlanabilmesi için ayrıca güvenlik duvarı, IDS/IPS, SIEM, SOAR, XDR, DLP gibi güvenlik cihazlarından da önemli ölçüde faydalanılmaktadır. Bu cihazlar ağ içindeki trafiği analiz ederek olası bir şüpheli durumda müdahale edebilmekte ya da ağ yöneticisini alarm sistemiyle bilgilendirebilmektedir.

İşletmeler, kapsamlı siber güvenlik önlemlerini uygulayarak kaynaklarını koruyabilir ve yetkisiz erişimi veya kötü niyetli faaliyetleri önleyebilir. Ağ güvenliğinin etkin bir şekilde sağlanabilmesi için çeşitli periyotlarda zafiyet analizi ve sızma testi yapılması büyük önem teşkil etmektedir.

2.2.4 Uygulama güvenliği

Uygulama güvenliği, yazılım uygulamalarını güvenlik açıklarından ve saldırılardan korumak için uygulanan önlem ve uygulamaları ifade eder. Uygulama verilerinin ve işlevselliğinin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için potansiyel risklerin tanımlanmasını ve azaltılmasını içerir. Web uygulamalarının güvenliğini sağlamak, uygulama güvenliğinin kritik bir yönüdür.

Web uygulamaları, kritik hizmetlerde kullanımının artması nedeniyle güvenlik saldırılarının popüler hedefleri haline gelmiştir (Li ve Xue, 2014). Sunucu taraflı güvenlik yaklaşımları, web uygulamalarının güvenliğinin sağlanmasında önemli bir rol oynamaktadır ve bu bağlamda güvenlik açıklarını gidermek için çeşitli teknikler ve çerçeveler geliştirilmiştir.

Web uygulamalarının barındırılmasında sıkça kullanılan bulut bilişim, uygulama güvenliği açısından çeşitli zorluklar getirmektedir. İşletmelerin bulut hizmetlerine giderek daha fazla güvenmesiyle birlikte, bulutta barındırılan uygulamaların güvenliğinin sağlanması daha farklı yöntemlerin uygulanması zorunluluğunu beraberinde getirmektedir (Ramachandran ve Chang, 2014). Bulut kurumsal güvenliğine yönelik öneriler, kontrol listeleri ve en iyi uygulamalar, bulut ortamlarındaki riskleri azaltmak ve hassas verileri ve uygulamaları korumak için önem teşkil etmektedir.

2.2.5 Bulut güvenliği

Bulut güvenliği, bulut bilişim ortamlarındaki verilerin ve kaynakların korunmasını ve bütünlüğünü sağlamanın önemli bir parçasıdır. Bulut güvenliğinin önemli bir yönü, insan hatalarının ve yanlış yapılandırma açıklarının belirlenmesi ve

azaltılmasıdır. Bu faktörler genellikle bulut altyapısındaki siber saldırılara ve veri ihlallerine katkıda bulunur (Torkura vd., 2020). Uygun güvenlik önlemlerinin ve en iyi uygulamaların uygulanması bu risklerin azaltılmasına yardımcı olmaktadır.

Bulut güvenliği yönetişimi, bulut güvenliği zorluklarını yönetmenin bir diğer bileşenidir. Özellikle düzenlenmiş endüstrilerde kurumsal varlıkların ve itibarın korunmasını sağlamak için politikalar, prosedürler ve kontroller oluşturmayı içerir. Etkili bulut güvenliği yönetişim çerçevelerinin uygulanması, işletmelerin güvenlik risklerini ele almasına ve ilgili düzenlemelere uymasına yardımcı olmaktadır (Amah vd., 2023).

Güvenlik açığı risk yönetimi, bulut güvenliğinin kritik bir unsurudur. Bulut sağlayıcılarının, hizmetlerinin güvenlik güvence düzeylerini sağlamak için güvenlik açıklarını değerlendirmesi ve yönetmesi gerekir (Ahmadi vd., 2021). Bulut güvenliği için teknik güvenlik önlemleriyle birlikte risk analizinin yapılması da büyük ölçüde fayda sağlamaktadır. Bulut bilişimle ilişkili risklerin değerlendirilmesi ve anlaşılması, etkili güvenlik önlemlerinin uygulanmasına yardımcı olmaktadır (Zainuddin vd., 2020).

Tehdit modelleme, bulut bilişim ortamlarının güvenliğini sağlamaya yönelik başka bir yaklaşımdır. İşletmeler, potansiyel tehditleri ve güvenlik açıklarını belirleyerek, kritik bilgileri korumak ve veri gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için uygun karşı önlemler geliştirebilir (Amini vd., 2015). Bulut güvenliği için gizlilik ve veri güvenliği de bir başka dikkat edilmesi gereken konudur.

Hassas verilerin korunması ve güvenli depolama ve iletimin sağlanması bulut bilişim güvenliğinin olmazsa olmazlarındandır. Ayrıca, şifrelemenin, erişim kontrol mekanizmalarının ve güvenli uygulama mimarilerinin uygulanması, bulutta veri güvenliğini sağlamanın kilit noktalarıdır (Sun vd., 2014).

2.2.6 Nesnelerin interneti güvenliği

Nesnelerin İnterneti (IoT), otomotiv, aviyonik, otomasyon, enerji ve denizcilik gibi çeşitli alanlarda devrim yaratma potansiyeline sahip, hızla büyüyen ve dönüştürücü bir kavramdır. Birlikte çalışabilir bilgi ve iletişim teknolojilerine dayalı olarak fiziksel ve sanal şeyleri birbirine bağlayarak gelişmiş hizmetleri mümkün

kılan sensör, gömülü, bilgi işlem ve iletişim teknolojilerinin entegrasyonu olarak tanımlanmaktadır (Swamy ve Raju, 2020).

Nesnelerin İnterneti, tedarik zinciri içindeki bireysel birimlerin daha fazla esneklik ve yanıt verme yeteneği elde etmek için birbirleriyle iletişim kurduğu, daha yalın üretim ve daha düşük üretim maliyetlerine yol açan, daha birbirine bağlı üretim süreçlerine akıllı bir geçişi temsil etmektedir (Lam vd., 2020).

IoT'nin entegrasyonu aynı zamanda iletişim verimliliği, veri güvenliği, kullanıcı gizliliği ve sürdürülebilirlik gibi önemli zorlukları da beraberinde getirmektedir (Nižetić vd., 2020). IoT'nin yaygınlaşmasıyla ilgili en büyük endişelerden biri güvenlik ve gizlilik sorunlarıdır. Karmaşık güvenlik sorunları, verilerin düşük güçlü ve kayıplı ortamlarda iletilmesinden kaynaklanmakta, yetkisiz gözetime, kontrolsüz veri üretimine ve kullanımına, yetersiz kimlik doğrulamaya ve bilgi güvenliği risklerine yol açmaktadır (Youm, 2017).

Denizcilik sektörü IoT teknolojilerinin entegrasyonuyla önemli bir dönüşüm geçirmiştir. Denizcilikte Nesnelerin İnterneti (MIoT) kavramı, küresel ölçekte denizcilik ortamında kullanılan cihazlara her yerde bağlantı sağlamak, denizde emniyet ve güvenlik, çevre koruma ve araştırma ile ilgili hizmetleri geliştirmek için geliştirilmiştir. MIoT'nin, su altı hesaplama ve otonom su altı araçları (AUV'ler) için yörünge tasarımı gibi çeşitli denizcilik faaliyetlerini desteklemek için çok önemli bir kolaylaştırıcı olduğu öngörülmektedir (Hou ve diğerleri, 2023).

Uluslararası Denizcilik Örgütü, denizcilik endüstrilerini modernleştirmek için e-Navigasyon olarak bilinen MIoT kavramını başlatmıştır. Bu girişim, otonom nakliye, navigasyon, izleme ve diğer kritik operasyonlardaki uygulamalar dahil olmak üzere IoT'nin faydalarını denizcilik alanına genişletmeyi amaçlamaktadır (Zhang vd., 2020). MIoT aynı zamanda denizdeki çevre izleme, su altı biyolojik izleme, taktik izleme ve su ürünleri yetiştiriciliği izleme için umut verici bir navigasyon bilgi tekniği olarak da tanımlanmıştır (Qian, 2022).

MIoT'nin entegrasyonu, özellikle su altı ortamında güvenli ve güvenilir bir iletişim sistemine duyulan ihtiyaç da dahil olmak üzere çeşitli zorluklarla karşı karşıyadır. Sualtı Nesnelerinin İnterneti'nin (IoUT) gelişimi, deniz ve su altı ortamlarındaki su altı nesnelerini birbirine bağlamak için tasarlanmış, Gemilerin

İnterneti ve gemiden su altına IoT gibi yeni ortaya çıkan kullanım senaryolarını sunan, yeni ortaya çıkan bir iletişim ekosistemidir.

2.2.7 Operasyonel güvenlik

Siber güvenlik kontekstinde operasyonel güvenlik, bir işletmenin bilgi sistemleri ve ağlarının günlük operasyonlarını korumak için uygulanan önlem ve uygulamaları ifade etmektedir. Verilerin ve kaynakların gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanmasının yanı sıra yetkisiz erişime, kesintilere ve saldırılara karşı koruma sağlamaktadır. Operasyonel güvenliğin bir yönü, veri ve iletişimin güvenliğini sağlamak için kriptografik protokollerin ve algoritmaların uygulanmasını da içermektedir.

Kriptografi, hassas bilgilerin korunmasında ve güvenli iletim ve depolamanın sağlanmasında önemli bir rol oynamaktadır. Kriptografi sayesinde veriler, ele geçirilse dahi şifrelenmiş olduğundan çözümlenememektedir. Siber güvenlik farkındalığı ve risk yönetimi de operasyonel güvenliğin önemli bileşenleridir. Kullanıcıları potansiyel güvenlik riskleri konusunda eğitmek ve güvenli güvenlik uygulamalarını teşvik etmek, güvenlik açıklarının azaltılmasına ve genel operasyonel güvenliğin geliştirilmesine yardımcı olmaktadır (Singgalen vd., 2021).

Siber güvenlik ile kurumsal risk yönetimini (ERM) entegre etmek, operasyonel güvenliğe yönelik başka bir yaklaşımdır. İşletmeler, siber güvenlik risklerini genel risk yönetimi stratejilerinin bir parçası olarak dikkate alarak operasyonlarını ve varlıklarını korumak için bilinçli kararlar alabilir (Stine vd., 2020).

Siber güvenlik operasyonlarında durumsal farkındalık, operasyonel güvenlik açısından da önemlidir. Siber güvenlik ortamının mevcut durumunu ve potansiyel tehditleri anlamak, kuruluşların risklere proaktif bir şekilde yanıt vermesine ve bunları azaltmasına imkan sağlamaktadır.

Siber güvenlikte operasyonel güvenlik aynı zamanda operasyonel teknolojilerin sertifikalandırılmasını ve düzenlenmesini de içerir (Tsvilii, 2021). Siber güvenlik sertifikasyon programlarının uygulanması ve düzenleyici çerçevelere bağlı kalınması, operasyonel sistemlerin güvenliğinin sağlanmasına metodolojik yaklaşım getirmektedir.

2.2.8 Felaketten kurtarma ve iş sürekliliği

Felaketten kurtarma ve iş sürekliliği planlaması, potansiyel felaketler karşısında kurumsal hazırlığın temel bileşenleridir. BT uzmanları için iş sürekliliği ve felaket kurtarma planlaması, bir felaket durumunda hayati fonksiyonların sürekli çalışmasını sağlamaya ve varlıkları korumaya yönelik strateji ve önlemleri içerir (Snedaker, 2007).

İşletmelerin felaketten kurtarma çalışmalarına rehberlik etmek için çeşitli felaket kurtarma çerçeve ve modelleri önerilmiştir (Mohamed, 2014). Yerinde, ortak yerleşim veya bulut çözümleri gibi felaket kurtarma alternatiflerinin işletme BT altyapısı dahilinde entegre edilmesi gerekmektedir. Bu sistemler ayrıca belirli dönemlerde test edilmeli, saldırı simülasyonları yapılarak kurtarma operasyonları tatbik edilmelidir.

İş sürekliliği yönetimi, geleneksel felaket kurtarma planlamasından bir ilerleme olarak görülmektedir. Felaket kurtarma stratejisi seçimine yardımcı olmak için ampirik modeller ve acil durum planlama yaklaşımları geliştirilmiştir (Wiboonrat, 2008). Genel olarak felaket kurtarma ve iş sürekliliği planlaması, işletmelerin olası felaketler karşısında operasyonlarının dayanıklılığını ve sürekliliğini sağlamaları açısından kritik öneme sahiptir. Ayrıca; felaket öncesi hazırlık iş sürekliliği ve felaket sonrası toparlanma açısından değerlendirilmesi gereken faktörlerdir.

2.2.9 İnsan faktörü ve eğitim

Siber güvenlikte insan faktörü, insan davranışının, tutumlarının ve eylemlerinin bilgi sistemleri ve ağlarının güvenliğinde oynadığı rolü ifade eder. Siber güvenlik ortamında insanların hem potansiyel risk oluşturucular hem de risk azaltıcılar olduğunu kabul etmektedir (King vd, 2018). Araştırmalar dürtüsellik, siber güvenliğe yönelik tutumlar ve riskli siber güvenlik davranışları gibi insan faktörlerinin siber tehdit olasılığını etkileyebileceğini göstermiştir (Hadlington, 2017).

İnsan faktörünü anlamak, etkili siber güvenlik stratejileri geliştirmek ve güvenlik açıklarını azaltmak için çok önemlidir. Siber güvenlikte insan faktörünün bir yönü de son kullanıcıların farkındalığı ve eğitimidir. Son kullanıcı siber farkındalık eğitimi, bireyleri siber güvenlik riskleri, en iyi uygulamalar ve güvenlik

protokollerini takip etmenin önemi konusunda eğitmeyi amaçlamaktadır (Antunes vd., 2021).

Kullanıcıların kimlik avı saldırıları veya sosyal mühendislik gibi potansiyel tehditleri tanımasına yardımcı olur ve kendilerini ve kuruluşlarını korumak için bilinçli kararlar almalarını sağlar (Matheu vd., 2020). İşletmeler, son kullanıcı farkındalığını artırarak, güvenlik ihlallerine yol açabilecek insan hatası veya ihmal olasılığını azaltabilir (Khamzina vd., 2022).

Siber güvenlikte insan faktörünün bir diğer boyutu da insan zafiyetlerinin siber güvenliğe etkisidir. Stres, tükenmişlik ve güvenlik yorgunluğu gibi faktörler, bireylerin güvenlik protokollerine uyma ve sağlam siber güvenlik kararları verme becerilerini etkileyebilir (Nobles, 2022). Ayrıca bireylerin siber güvenlik farkındalığı ve bilgi eksikliği, onları siber tehditlere karşı daha duyarlı hale getirebilmektedir (Nobles, 2018). Bu güvenlik açıklarının eğitim, destek ve işletme kültürü yoluyla ele alınması, siber güvenlik savunmalarının güçlendirilmesine yardımcı olabilir.

İnsan faktörü aynı zamanda siber güvenlik sistemlerinin tasarımına ve kullanılabilirliğine de uzanır. İnsan merkezli tasarım ilkeleri, güvenlik önlemlerinin kullanılabilirliğini ve etkinliğini artırarak bireylerin güvenlik protokollerine uymasını kolaylaştırabilir (Hadlington, 2018).

Güvenlik arayüzleri ve sistemleri tasarlanırken son kullanıcıların bilişsel yükünün ve sınırlamalarının dikkate alınması, onların güvenli seçimler yapma yeteneklerini geliştirebilir (Adu ve Adjei, 2018). Dahası, siber güvenlik teknolojilerinin benimsenmesi ve kullanılmasında yer alan insan faktörlerinin anlaşılması, kullanıcı dostu ve etkili güvenlik çözümlerinin geliştirilmesine bilgi sağlayabilir (Rajamäki ve Järvinen, 2022).

2.2.10 Siber tehditler

Siber tehditler bireyler, işletmeler ve hatta bir bütün olarak toplum için önemli riskler oluşturmaktadır. Bilgi sistemleri ve ağlarındaki güvenlik açıklarından yararlanan çok çeşitli kötü amaçlı etkinlikleri kapsarlar. Denizcilik sektöründeki modern tehditler ve trendlerin sistematik bir incelemesi, siber tehditlerin gelişen doğasını ve artan siber güvenlik önlemlerine duyulan ihtiyacı vurgulamaktadır.

Siber tehditlerde insan faktörü çok önemli bir rol oynamaktadır. Denizcilik işletmelerinde insan faktörlerinin siber güvenlik üzerindeki etkisine ilişkin sistematik bir inceleme, insani güvenlik açıklarının siber saldırganlar tarafından istismar edilebileceğini ortaya koymaktadır. Bu, yetkisiz erişim elde etmek veya güvenlik sistemlerini tehlikeye atmak için insan davranışlarından, tutumlarından ve eylemlerinden yararlanmayı içermektedir.

Siber tehditlerle etkili bir şekilde mücadele etmek için siber tehdit istihbaratı alanı ortaya çıkmıştır. Bu, proaktif siber güvenlik önlemlerini bilgilendirmek için mevcut veya potansiyel tehditler hakkında kanıta dayalı bilgilerin toplanmasını içerir. Siber tehdit istihbarat modelleri ve çerçeveleri, kuruluşların tehditleri zamanında ve etkili bir şekilde değerlendirmesine ve bunlara yanıt vermesine yardımcı olmaktadır (Mavroeidis ve Bromander, 2017).

Yapay zeka ve doğal dil işleme gibi teknolojideki ilerlemelerden de siber tehditlerin tanımlanması ve profilinin çıkarılması için yararlanılmaktadır. Akıllı veri analizine ve makine öğrenimi tekniklerine dayanan otomatik yöntemler, siber tehditlerin tespit edilmesine ve tahmin edilmesine yardımcı olmaktadır (Marinho ve Filho, 2023). Bu yaklaşımlar potansiyel tehditlerin erken tespit edilmesini ve bunlara yanıt verilmesini sağlayarak genel siber güvenlik direncini artırmaktadır.

2.2.10.1 Zararlı yazılım (Malware)

Zararlı yazılım, ağlara veya cihazlara yetkisiz erişim sağlamak, zarar vermek veya bunlara zarar vermek amacıyla kötü niyetli olarak tasarlanmış herhangi bir yazılım veya kodu ifade eder. Virüsler, solucanlar, Truva atları, fidye yazılımları, casus yazılımlar, reklam yazılımları ve daha fazlası dahil olmak üzere çok çeşitli tehditleri kapsar (Kothawade, 2022).

Zararlı yazılım, e-posta ekleri, virüslü web siteleri, çıkarılabilir medya veya yazılım indirmeleri gibi çeşitli yollarla yayılabilir (Peng vd., 2014). Zararlı yazılım, bir sisteme yüklendikten sonra hassas bilgileri ele geçirmek, sistem bütünlüğünü tehlikeye atmak veya normal işlemleri bozmak gibi çeşitli kötü amaçlı faaliyetler gerçekleştirebilir.

Zararlı yazılımlar, bilgisayar sistemlerindeki ve ağlarındaki güvenlik açıklarından yararlanarak genellikle yazılımdaki veya insan davranışındaki zayıflıkları hedef almaktadır. Siber suçlular, tespit edilmekten kaçınmak ve etkilerini

en üst düzeye çıkarmak için kötü amaçlı yazılım tekniklerini sürekli olarak geliştirmektedir (Kolosnjaji ve diğerleri, 2018). Kötü amaçlı yazılımların tespit edilmesini ve analiz edilmesini zorlaştırmak için gizleme teknikleri, şifreleme veya polimorfizm kullanabilirler (Aslan ve Samet, 2020). Ek olarak kötü amaçlı yazılım, kullanıcıları kötü amaçlı dosyaları çalıştırmaya veya indirmeye kandırmak için sosyal mühendislik taktiklerinden yararlanabilir (Li ve diğerleri, 2017).

Zararlı yazılımın etkisi ciddi olabilir; finansal kayıplara, veri ihlallerine, gizlilik ihlallerine ve bireyler ile kuruluşların itibarının zarar görmesine neden olabilir. Zararlı yazılım saldırıları kritik altyapıyı bozabilir, hassas bilgileri tehlikeye atabilir ve önemli operasyonel kesintilere neden olabilir (Liu ve Zhong, 2017). Zararlı yazılımların gelişen doğası, ortaya çıkan tehditleri tespit etmek ve azaltmak için savunmalarını sürekli olarak güncellemesi gereken siber güvenlik profesyonelleri için önemli bir zorluk teşkil etmektedir (Aslan ve Samet, 2020).

Zararlı yazılımlarla mücadele etmek için antivirüs yazılımı, izinsiz giriş tespit sistemleri, güvenlik duvarları ve davranış tabanlı analiz dahil olmak üzere çeşitli teknikler ve teknolojiler kullanılmaktadır. Zararlı yazılımları kalıplara ve özelliklere göre tespit etmek ve sınıflandırmak için makine öğrenimi ve yapay zeka algoritmaları da kullanılmaktadır (Senanayake vd., 2021).

Günümüzde, zararlı yazılım geliştiricileri ile siber güvenlik uzmanları arasındaki kedi-fare oyunu, yeni kötü amaçlı yazılım çeşitleri ve kaçırma tekniklerinin sürekli ortaya çıkmasıyla devam etmektedir (Han vd., 2018). Gelişen yapay zeka teknolojileri sayesinde zararlı yazılım algoritmaları da karmaşıklaşmakta, böylelikle daha zor tespit edilebilen ve daha yüksek etki kapasitesine sahip saldırılar düzenlenebilmektedir.

2.2.10.2 Virüsler

Virüs, kendini çoğaltmak ve bir bilgisayar sisteminden diğerine yayılmak üzere tasarlanmış bir tür kötü amaçlı yazılımdır. Kendini meşru dosyalara veya programlara bağlar ve virüslü dosya veya program çalıştırıldığında kötü amaçlı kodunu çalıştırabilir. Virüsler genellikle virüslü e-posta ekleri, indirilen dosyalar veya USB sürücüler gibi çıkarılabilir ortamlar aracılığıyla yayılır. Bir virüs bir sisteme bulaştığında veri bozulması, sistem çökmesi veya hassas bilgilere yetkisiz erişim gibi bir dizi zararlı etkiye neden olabilir (Mylonas ve Gritzalis, 2012).

Virüsler, genellikle bilgisayar sistemlerindeki veya insan davranışındaki güvenlik açıklarından yararlanarak kendi kendini kopyalama ve yayılma yetenekleriyle karakterize edilir. Davranışlarına ve yayılma yöntemlerine göre farklı türlere sınıflandırılabilirler. Bazı virüsler dosyaların üzerine yazmak veya değiştirmek üzere tasarlanmışken, bazıları sistemde gizlenip hassas bilgileri sessizce toplayabilir (Balthrop vd., 2004). Virüslerin yayılması, ağ bağlantıları, e-posta ağları veya dosya paylaşım platformları gibi çeşitli yollarla gerçekleşebilir. Virüslerin evrimi, tespit edilmekten kaçınmak için kodlarını değiştirebilen polimorfik virüsler gibi daha karmaşık tekniklerin geliştirilmesine yol açmıştır.

Virüsleri tespit etmek ve etkilerini azaltmak, antivirüs yazılımının kullanılmasını ve güvenlik açıklarını düzeltmek için düzenli sistem güncellemelerini gerektirir. Antivirüs yazılımı, enfeksiyonları tanımlamak ve kaldırmak için dosyaları ve programları bilinen virüs imzalarına veya şüpheli davranışlara karşı tarar. Ancak virüslerin sürekli evrimi, antivirüs yazılımları için bir zorluk teşkil etmektedir. Yeni ve bilinmeyen virüsler hemen tespit edilemeyebilir. Bu durum, antivirüs yazılımını güncel tutmanın ve şüpheli indirmelerden kaçınmak veya bilinmeyen e-posta eklerini açmak gibi güvenli bilgisayar kullanma alışkanlıklarını uygulamanın önemini vurgulamaktadır (Regenmortel ve Mahy, 2004).

Virüslerin etkisi işletmeler için oldukça ciddidir; mali kayıplara, veri ihlallerine ve iş operasyonlarında aksamalara neden olabilir. İşletmeler, virüslere ve diğer kötü amaçlı yazılım tehditlerine karşı koruma sağlamak için derinlemesine savunma önlemleri uygulamalıdır. Bu gelişmiş savunma, önemli verilerin düzenli olarak yedeklenmesini, güçlü şifre yönetimini ve güvenli bilgi işlem uygulamaları konusunda kullanıcı eğitimini içerir (Sáez-López vd., 2019). Ek olarak, güvenlik duvarları ve izinsiz giriş tespit sistemleri gibi ağ güvenlik önlemleri, ağ içinde virüslerin yayılmasını önlemeye yardımcı olabilir.

2.2.10.3 Truva atları

Yaygın olarak trojan olarak bilinen bilgisayar truva atı, kullanıcıları onu çalıştırmaya veya indirmeye ikna etmek için kendisini meşru bir program veya dosya olarak gizleyen bir tür kötü amaçlı yazılımdır. Virüslerden veya solucanlardan farklı olarak truva atları kendi kendine çoğalmaz. Bunun yerine, bir bilgisayar sistemine

veya ağına yetkisiz erişim sağlamak için sosyal mühendislik taktikleri veya yazılımdaki güvenlik açıklarından yararlanmaktadır.

Truva atları, e-posta ekleri, yazılım indirmeleri veya güvenliği ihlal edilmiş web siteleri gibi çeşitli yollarla dağıtılabilir. Bir truva atı yürütüldüğünde hassas bilgileri çalmak, saldırganlara uzaktan erişim sağlamak veya ek kötü amaçlı yazılım yüklemek gibi bir dizi kötü amaçlı etkinlik gerçekleştirebilir (Dou vd., 2021).

Truva atları, amaçlarına veya davranışlarına göre farklı türlere ayrılabilir. Örneğin, bir truva atı, bir sisteme yetkisiz erişim sağlayan bir arka kapı görevi görebilir veya hassas bilgileri yakalamak için tuş vuruşlarını kaydeden bir tuş kaydedici olarak işlev görebilir. Bazı truva atları özellikle finansal bilgileri hedeflemek için tasarlanmışken diğerleri casusluk veya veri hırsızlığına odaklanabilir. Truva atlarının çok yönlülüğü ve uyarlanabilirliği, onları sistemleri tehlikeye atmak veya hassas verilere yetkisiz erişim elde etmek isteyen siber suçlular için popüler bir seçim haline getirmektedir.

Truva atlarını tespit etmek ve etkilerini azaltmak, aldatıcı doğaları nedeniyle zor bir çalışma gerektirebilmektedir. Antivirüs yazılımları ve diğer güvenlik araçları, truva atlarını tanımlamak ve kaldırmak için imza tabanlı algılama, davranış analizi veya sezgisel tarama gibi çeşitli teknikler kullanır (Kanaker vd., 2022). Ancak truva atlarının sürekli gelişmesi ve gizleme tekniklerinin kullanılması, tüm varyantların tespit edilmesini zorlaştırmaktadır.

Düzenli yazılım güncellemeleri, güçlü şifre yönetimi ve güvenli bilgi işlem uygulamaları konusunda kullanıcı eğitimi, truva atı enfeksiyonlarını önlemek için önemlidir. Ek olarak, güvenlik duvarları ve izinsiz giriş tespit sistemleri gibi ağ güvenliği önlemleri, truva atı aktivitesinin tespit edilmesine ve engellenmesine yardımcı olabilir.

2.2.10.4 Casus yazılım

Casus yazılım, kullanıcının bilgisi veya rızası olmadan, kullanıcının etkinlikleri hakkında gizlice bilgi toplamak için tasarlanmış bir tür kötü amaçlı yazılımdır. Genellikle kullanıcının haberi olmadan bir bilgisayar sistemine kurulur ve genellikle yasal yazılımlarla birlikte veya aldatıcı taktiklerle paketlenir.

Casus yazılım yüklendikten sonra kullanıcının çevrimiçi etkinliklerini izleyebilir, tuş vuruşlarını izleyebilir, oturum açma kimlik bilgileri veya finansal veriler gibi hassas bilgileri yakalayabilir ve bu bilgileri uzaktaki bir saldırgana iletebilir (Dinev ve Hu, 2007). Casus yazılımlar, genellikle kimlik hırsızlığı, yetkisiz gözetim veya hedefli reklamcılık gibi kötü amaçlarla kullanılır.

Casus yazılımlar, virüslü e-posta ekleri, kötü amaçlı web siteleri veya güvenilmeyen kaynaklardan indirilen yazılımlar dahil olmak üzere çeşitli yollarla dağıtılabilir (Buil-Gil vd., 2021). Bir kullanıcının sistemine yetkisiz erişim sağlamak için web tarayıcılarındaki, işletim sistemlerindeki veya diğer yazılımlardaki güvenlik açıklarından yararlanabilir. Casus yazılımlar, kullanıcıları yanıltıcı bağlantılara tıklamaya veya görünüşte zararsız dosyalar indirmeye ikna etmek gibi sosyal mühendislik taktikleri yoluyla da yayılabilir (Miraja vd., 2019). Casus yazılım yüklendikten sonra arka planda sessizce çalışır ve kullanıcıların varlığını tespit etmesini zorlaştırır.

Casus yazılımın etkisi işletmeler açısından önemlidir; kullanıcı gizliliğini, güvenliğini ve sistem performansını tehlikeye atabilir. Dahası kimlik hırsızlığına, mali kayba veya hassas bilgilere yetkisiz erişime yol açabilir. Casus yazılımlar ayrıca sistem performansını düşürebilir, ağ bant genişliğini tüketebilir ve sistem çökmelerine veya kararsızlığa neden olabilir (Sarker ve diğerleri, 2021). Casus yazılımların kaldırılması bazı durumlarda zor olabilir. Antivirüs yazılımları veya güvenlik araçları tarafından tespit edilmekten kaçınmak için genellikle gizli teknikler kullanılır (Wang vd., 2021).

Casus yazılımlara karşı korunmak için kullanıcıların çeşitli önleyici tedbirler alması gerekir. Bunlar, güvenlik açıklarını düzeltmek için işletim sistemlerini ve yazılımları düzenli olarak güncellemeyi, saygın antivirüs ve casus yazılım önleme yazılımlarını kullanmayı ve dosyaları indirirken veya bilinmeyen veya güvenilmeyen kaynaklardan gelen bağlantılara tıklarken dikkatli olmayı içerir (Kimpe vd., 2020).

Şüpheli web sitelerinden kaçınmak, pop-up reklamlara tıklamamak ve kişisel bilgileri çevrimiçi paylaşırken dikkatli olmak gibi güvenli gezinme alışkanlıklarını uygulamak da önemlidir (Howah ve Chugh, 2019). Düzenli sistem taramaları ve olağandışı sistem davranışlarının izlenmesi, casus yazılım bulaşmalarının tespit edilmesine ve kaldırılmasına yardımcı olabilir (Thatcher vd., 2007).

2.2.10.5 Fidye yazılım

Fidye yazılım, saldırgana bir fidye ödenene kadar kurbanın dosyalarını şifreleyen veya bilgisayar sistemlerinden kilitleyen, genellikle Bitcoin gibi kripto para birimi cinsinden ödeme kabul edildikten sonra, siber saldırganlar tarafından devre dışı bırakılan bir tür kötü amaçlı yazılımdır (Paquet-Clouston vd., 2019). Fidye yazılım saldırıları genellikle yazılımdaki güvenlik açıklarından yararlanır veya kullanıcıları kötü amaçlı yazılımı indirmeleri veya çalıştırmaları için kandırmak amacıyla sosyal mühendislik taktiklerini kullanır (Scalas vd., 2019).

Fidye yazılım bulaştığında kurbanın dosyaları şifrelenir ve fidye ödenene ve şifre çözme anahtarı sağlanana kadar dosyalara erişilemez hale gelir (Rawindaran vd., 2021). Fidye yazılım saldırıları giderek daha yaygın ve karmaşık hale gelmiştir ve denizcilik sektörü ile birlikte, sağlık kurumları, devlet kurumları ve her büyüklükteki sair işletmeleri dahil olmak üzere çok çeşitli kurbanları hedef almaktadır (Beaman vd., 2021). Fidye yazılım saldırılarının mali etkisi çok büyük olmaktadır. Kurbanlar yalnızca fidye maliyetiyle değil aynı zamanda potansiyel veri kaybı, kesinti, itibar kaybı ve yasal sonuçlarla da karşı karşıya kalmaktadır (August vd., 2022).

Kripto para birimlerinin yükselişi, ödemeleri de zorlaştırmaktadır. Kripto paraların anonimliğe müsaade etmesi de talep edilen ya da gerçekleştirilen ödemelerin izlenmesini ve kurtarılmasını daha zor hale getirmektedir (Kapoor vd., 2021). Fidye yazılımın tehdidini azaltmak için çok katmanlı bir yaklaşım uygulamak gerekmektedir. Önleme tedbirleri arasında yazılım ve işletim sistemlerinin düzenli olarak güncellenmesi, gelişmiş güvenlik çözümlerinin uygulanması ve kullanıcıların güvenli bilgi işlem uygulamaları konusunda eğitilmesi yer almaktadır (Conti vd., 2018).

Yedekleme sistemleri ve felaket kurtarma planları, bir saldırı durumunda verileri geri yüklemek için çok önemlidir (Haner vd., 2022). Tespit ve müdahale stratejileri, ağ trafiğinin izlenmesini, davranışa dayalı analizin kullanılmasını ve daha fazla yayılmayı önlemek için virüslü sistemlerin derhal izole edilmesini içerir (McDonald vd., 2022). Siber güvenlik uzmanları, kolluk kuvvetleri ve devlet nezdinde karar alıcılar arasındaki işbirliği de küresel ölçekte fidye yazılımlarıyla mücadele için çok önemlidir (Warikoo, 2023).

2.2.10.6 Reklam yazılımı

Reklam yazılımı, kullanıcının bilgisayarında veya mobil cihazında istenmeyen reklamlar görüntüleyen yazılımları ifade eder. Genellikle yasal yazılımlarla birlikte gelir ve kullanıcının açık rızası olmadan yüklenir. Reklam yazılımları genellikle hedefli reklamlar görüntüleyerek veya reklam amaçlı kullanıcı verilerini toplayarak yaratıcıları için gelir elde eder (Sarker, 2020). Bazı reklam yazılımları nispeten zararsız olsa da diğerleri müdahaleci, yıkıcı ve hatta kötü niyetli olabilir.

Reklam yazılımları, açılır reklamlar, afişler veya web sayfalarına reklam enjekte eden tarayıcı uzantıları dahil olmak üzere çeşitli biçimlerde ortaya çıkabilir. Ayrıca kullanıcıları istenmeyen web sitelerine yönlendirebilir veya izinsiz olarak tarayıcı ayarlarını değiştirebilir (Sihwail vd., 2018). Reklam yazılımları, kullanıcı davranışını izlemek ve toplanan verilere dayalı olarak kişiselleştirilmiş reklamlar görüntülemek için genellikle izleme teknolojilerinden yararlanır. Bazı durumlarda reklam yazılımları, hassas bilgileri izinsiz toplayarak veya üçüncü taraflara ileterek kullanıcının gizliliğini tehlikeye atabilir (Liu vd., 2022).

Reklam yazılımının etkisi, kullanıcı deneyiminin rahatsız edilmesinden ve kesintiye uğramasından potansiyel güvenlik risklerine kadar değişebilir. Reklam yazılımları sistem performansını yavaşlatabilir, ağ bant genişliğini tüketebilir ve uygulamaların ve web tarayıcılarının normal işleyişine müdahale edebilir (Kanaker vd., 2022). Ek olarak, bazı reklam yazılımları, casus yazılım veya fidye yazılımı gibi diğer kötü amaçlı yazılım türlerini dağıtmak için bir araç görevi görebilir (Dambra vd., 2023). Kalıcı mekanizmalar kullanabilecekleri veya sistem dosyaları içinde gizlenebilecekleri için reklam yazılımlarının sistemden kaldırılması zor olabilir.

Reklam yazılımlarına karşı korunmak için kullanıcılar, güvenilmeyen kaynaklardan yazılım indirirken dikkatli davranmalı ve kurulum sırasında hüküm ve koşulları dikkatle incelemelidir. Gizlilik politikalarını okumak ve kişisel verilerin yazılım uygulamaları tarafından nasıl toplanabileceğini ve kullanılabileceğini anlamak önemlidir.

Gelişmiş antivirüs yazılımı ve reklam engelleme uzantılarının kullanılması, reklam yazılımlarının tespit edilmesine ve engellenmesine yardımcı olabilir (Wang vd., 2021). Düzenli sistem taramaları ve yazılım güncellemeleri, reklam

yazılımlarının yararlanabileceği güvenlik açıklarını kapatmak için önemli fayda sağlamaktadır.

2.2.10.7 Zombi bilgisayarlar ve botnetler

Zombi bilgisayarlar ve botnet'ler siber güvenlik alanında önemli tehditlerdir. Zombi bilgisayar, bir bilgisayar korsanı, virüs veya truva atı tarafından ele geçirilen ve kötü niyetli bir aktör tarafından kontrol edilen bir sistemi ifade eder (Sharma vd., 2014). Güvenliği ihlal edilen bu bilgisayarlar, botnet olarak bilinen zombi bilgisayar topluluğundan oluşturan koordineli saldırılar başlatmak için kullanılabilir.

Botnet, tek bir varlığın (Command Center) komutası altında olan ve denetleyicinin dağıtılmış hizmet reddi (DDoS) saldırıları ve kötü amaçlı yazılım yayma gibi çeşitli kötü amaçlı etkinlikleri yürütmesine olanak tanıyan, virüs bulaşmış bilgisayarlardan oluşan bir ağdır. Bu ağların toplu bir şekilde hedefe saldırması ile birlikte yıkıcı sonuçlar meydana gelebilir.

Botnet'lerin çoğalması, ağ güvenliği üzerindeki etkileri ve yaygın kesinti potansiyeli konusunda endişeleri artırmaktadır. Botnet'ler, koordineli saldırılar gerçekleştirmek için çok sayıda güvenliği ihlal edilmiş cihazdan yararlanarak giderek daha karmaşık bir yapıya kavuşmuş ve bu da onları yaygın bilgi işlem ve Nesnelerin İnterneti çağında önemli bir tehdit haline gelmiştir. Botnet'lerin birbirine bağlı doğası, geleneksel güvenlik önlemlerinden kaçabildikleri ve devlet kurumları, özel şirketler ve haneler dahil olmak üzere çeşitli sektörler üzerinde önemli olumsuz etkilere sahip olabildikleri için tespit ve hafifletme açısından zorluklar doğurmaktadır (Vu vd., 2021).

Botnet'lerin oluşturduğu tehdidi ele almak için araştırmacılar, bu kötü amaçlı ağlara karşı koruma sağlayacak algılama ve izolasyon mekanizmaları geliştirmelted,r. Spam tespitinin verimliliğini artırmayı ve zombi bilgisayarların oluşumunu önlemeyi amaçlayan, botnet etkisini belirlemek ve azaltmak için çeşitli tespit çerçeveleri ve modelleri önerilmiştir (Kumar ve Singh, 2017).

2.2.10.8 Structured query language (SQL) injection

SQL enjeksiyonu, kayıtları veritabanında saklayan web uygulamaları ve yazılımlar için önemli bir tehdit oluşturan yaygın bir güvenlik açığı türüdür. SQLi, herhangi bir giriş alanına kötü amaçlı SQL ifadeleri eklenmesi, hassas bilgilere

yetkisiz erişim elde etmesine ve keyfi komutlar yürütmesine olanak sağlamasıyla ortaya çıkmaktadır (Abdullayev ve Chauhan, 2023).

SQL enjeksiyon saldırılarına karşı koymak için çeşitli tespit ve önleme teknikleri önerilmiştir. Örneğin, gelişmiş SQL enjeksiyonlarını tespit etmek ve önlemek için makine öğreniminden yararlanılması, bu yaklaşımın bu tür saldırıların etkisini azaltma potansiyelini ortaya koymaktadır (Volkova vd., 2019). Web uygulamalarının SQL enjeksiyon saldırılarına kurban gitmesini önlemek için algılama modellerinin ve anormallik saldırı tespit sistemlerinin geliştirilmesi konusunda da çeşitli araştırmalar yapılmaktadır (Qbea'h ved., 2016).

SQL enjeksiyon saldırılarının ciddiyeti, web uygulamalarını korumak için savunma modellerinin ve tekniklerinin araştırılmasına yol açmıştır. Girdi alanlarını filtreleyerek, sözdizimi karşılaştırması ve parametre değiştirme yoluyla SQL enjeksiyonu riskini azaltmak için savunma modelleri olarak parametreleştirilmiş sorgular ve geliştirilmiş parametrelendirme önerilmektedir (Chen vd., 2018).

2.2.10.9 Kimlik avı saldırıları

Kimlik avı, bireyleri kişisel kimlik bilgileri, mali ayrıntılar veya diğer gizli veriler gibi hassas bilgileri ifşa etmeleri için kandırmak amacıyla aldatıcı taktiklerin kullanılmasını içeren yaygın bir siber saldırı biçimidir. Kimlik avı saldırısı, genellikle e-posta, anlık mesajlaşma veya dolandırıcılık amaçlı web siteleri aracılığıyla meydana gelen ve saldırganın kurbanı hassas bilgilerini vermesi için kandırmak amacıyla güvenilir bir varlık gibi davrandığı bir tür sosyal mühendislik saldırısıdır (Jampen vd., 2020). Kimlik avı saldırıları, hedeften bir yanıt almak için genellikle insanın zayıf noktalarından ve psikolojik manipülasyondan yararlanır ve bu da onu siber güvenlik alanında önemli bir tehdit haline getirir (Nifakos vd., 2021).

Kimlik avı saldırıları etkisi geniş kapsamlıdır ve hem bireyler hem de kuruluşlar için mali kayıplara, kimlik hırsızlığına ve itibar kaybına neden olur. Kimlik avı saldırıları, çevrimiçi etkileşimlerde güveni ve güvenliği zayıflattığından e-ticaret, bankacılık ve sosyal medya dahil olmak üzere çeşitli sektörler için büyük bir endişe kaynağıdır (Jampen vd., 2020).

Kimlik avı tehdidini ele almak amacıyla araştırmacılar, kimlik avı saldırılarını tespit etmek ve önlemek için makine öğrenimi, doğal dil işleme ve buluşsal tabanlı algoritmalar dahil olmak üzere bir dizi yaklaşım ortaya koymuştur.

Bu öneriler, sosyal mühendislik saldırılarının etkisini azaltmak için proaktif önlemlerin önemini vurgulayarak bireylerin ve kuruluşların kimlik avı girişimlerine karşı dayanıklılığını artırmayı amaçlamaktadır (Aydın vd., 2020).

Yapılan çalışmalar, siber güvenlik farkındalığı eğitiminin, dijital dürtüklemenin ve işbirlikçi öğrenme algoritmalarının kimlik avı saldırılarına karşı duyarlılığı azaltmadaki rolünü araştırmış ve bu tür siber suçlara karşı savunma stratejilerinin çok yönlü doğasını vurgulamaktadır (Back ve Guerette, 2021).

2.2.10.10 Ortadaki adam (MiTM) saldırısı

Ortadaki adam (MiTM) saldırısı, kötü niyetli bir aktörün birbirleriyle doğrudan iletişim kurduğuna inanan iki taraf arasındaki iletişimi kestiği ve potansiyel olarak değiştirdiği bir siber saldırı biçimidir. Saldırgan, iletişimi gizlice aktarır ve manipüle ederek, oturum açma kimlik bilgileri, finansal ayrıntılar veya kişisel veriler gibi hassas bilgileri gizlice dinleme ve ele geçirme olanağı elde eder (Mallik vd., 2019). Bu tür saldırılar, e-posta, anlık mesajlaşma ve çevrimiçi işlemler de dahil olmak üzere çeşitli iletişim kanallarında gerçekleşebilir ve değiştirilen bilgilerin gizliliği ve bütünlüğüne yönelik önemli bir tehdit oluşturabilir.

MiTM saldırılarının etkisi geniş kapsamlıdır ve bireyler ve kuruluşlar için potansiyel veri ihlallerine, kimlik hırsızlığına ve mali kayıplara yol açar. Saldırganlar, iletişim protokollerindeki veya ağ yapılandırmalarındaki güvenlik açıklarından yararlanarak kendilerini meşru taraflar arasında konumlandırabilir ve hassas bilgilere yetkisiz erişim elde ederek iletişim kanalının güvenliğini ve güvenilirliğini tehlikeye atabilir (Bıçakçı vd., 2014). MiTM saldırıları, kablosuz ağlar, çevrimiçi bankacılık, e-ticaret ve diğer dijital etkileşimler bağlamında büyük bir endişe kaynağıdır. Etkilerini azaltmak için güçlü önleme ve tespit mekanizmalarına ihtiyaç duyulmaktadır.

MiTM saldırılarına karşı korunmak için çeşitli karşı önlemler ortaya konulmaktadır. Bu yaklaşımlar arasında iletişim kanallarının orijinalliğini ve bütünlüğünü sağlamak ve böylece MiTM saldırılarına karşı duyarlılığı azaltmak için güvenli kimlik doğrulama protokolleri, şifreleme mekanizmaları ve dijital imzaların geliştirilmesi yer almaktadır. Bu yaygın tehditle mücadele etmek için gereken çok yönlü yaklaşımın vurgulanmasıyla, iletişim kanallarının potansiyel MiTM saldırılarına karşı dayanıklılığını güçlendirmek için güvenli cihaz eşleştirme

yöntemleri, gelişmiş şifreleme teknikleri ve izinsiz giriş tespit sistemlerinin kullanımı araştırılmıştır (Javeed vd., 2020).

2.2.10.11 Dağıtık hizmet reddi (DDoS) saldırıları

Dağıtık Hizmet Dışı Bırakma saldırıları olarak da tanımlanan Dağıtık Hizmet Reddi (DDoS) saldırıları, bir ağ hizmetini, cihazı veya web sitesini kötü niyetli trafik seli ile bunaltarak kullanılamaz hale getirmeyi amaçlayan yaygın ve yıkıcı bir siber saldırı biçimidir. Bu saldırılar, genellikle botnet olarak adlandırılan ve saldırganın kontrolü altındaki, güvenliği ihlal edilmiş cihazlardan oluşan bir ağ tarafından gerçekleştirilir. DDoS saldırılarının ölçeği ve dağıtılmış doğası, bunların azaltılmasını özellikle zorlaştırmaktadır. Bu saldırılar, önemli ağ kaynaklarını tüketebilir ve hedeflenen sistemlerin normal çalışmasını bozmaktadır (Zargar vd., 2013).

DDoS saldırılarının etkisi ciddi olup, hizmet kesintilerine, mali kayıplara ve kuruluşlar ile işletmeler için itibar kaybına neden olmaktadır. DDoS saldırıları, hedefi yüksek hacimli trafikle doldurarak ağ bant genişliğini tüketebilir, sunucu kaynaklarını tüketebilir ve çevrimiçi hizmetlerin kullanılabilirliğini bozabilir ve bu da potansiyel finansal ve operasyonel sonuçlara yol açabilir.

DDoS saldırıları tehdidine karşı, bu saldırılara karşı korunmak ve etkilerini azaltmak amacıyla çeşitli savunma mekanizmaları ve hafifletme teknikleri geliştirilmiştir. Bu önlemler, kötü amaçlı trafiği tanımlamak ve engellemek için trafik filtreleme, hız sınırlama ve anormallik tespitinin kullanımının yanı sıra, saldırı trafiğini absorbe etmek ve azaltmak için içerik dağıtım ağlarının (CDN'ler) ve bulut tabanlı DDoS koruma hizmetlerinin konuşlandırılmasını içerir (Mahjabin vd., 2017).

Ayrıca, ağ ve hizmetlerin DDoS saldırılarına karşı dayanıklılığını artırmak için makine öğrenimi tabanlı DDoS tespit sistemlerinin geliştirilmesi, ağ trafiği analiz araçlarının uygulanması ve güvenli kimlik doğrulama mekanizmalarının kullanımı araştırılmıştır. Bu çalışmalar, DDoS saldırılarını gerçek zamanlı olarak tespit etme ve bunlara yanıt verme yeteneğini geliştirmeyi, böylece hizmet kesintilerinin etkisini ve süresini azaltmayı amaçlamaktadır (Hariharan vd., 2019).

2.2.10.12 İçeriden gelen tehditler

Siber güvenlikte iç tehdit, bir kuruluş içindeki, kuruluşun sistemlerine, ağlarına veya verilerine erişim yetkisine sahip olan ve güvenliği tehlikeye atmak için bu erişimden yararlanabilecek kişilerin oluşturduğu riski ifade eder. Çalışanlar, yükleniciler veya ortaklar da dahil olmak üzere bu içerideki kişiler, kasıtlı veya kasıtsız olarak işletmeye ait bilgi varlıklarının gizliliğini, bütünlüğünü veya kullanılabilirliğini tehdit eden faaliyetlerde bulunabilir.

İçeriden gelen tehditler, geleneksel güvenlik önlemlerini atlayabildikleri ve bir işletmenin operasyonlarına, itibarına ve genel güvenlik duruşuna ciddi zararlar verebildiklerinden siber güvenlik açısından önemli bir endişe kaynağıdır (Probst vd., 2010). İçeriden gelen tehditlerin niteliği, veri hırsızlığı, sabotaj, dolandırıcılık veya yetkisiz erişim gibi bir dizi davranışı kapsayacak şekilde geniş çapta değişiklik gösterebilir. Bu tehditler finansal kazanç, intikam veya ideoloji gibi kişisel motivasyonların yanı sıra insan hatası, ihmal veya en iyi güvenlik uygulamalarına ilişkin farkındalık eksikliğinden de kaynaklanabilir.

İçeriden gelen tehditler, sosyal mühendislik saldırılarının kurbanı olmak, sistemleri yanlış yapılandırmak veya hassas bilgilerin yanlışlıkla ifşa edilmesi gibi kasıtsız eylemler şeklinde de ortaya çıkabilir. İçeriden gelen tehditleri azaltmak, teknik, organizasyonel ve insan odaklı stratejileri birleştiren çok yönlü bir yaklaşım gerektirir. Bu, erişim kontrollerinin uygulanmasını, kullanıcı etkinliklerinin izlenmesini ve denetlenmesini, güvenlik farkındalığı eğitiminin yürütülmesini ve açık güvenlik politikaları ve prosedürleri oluşturulmasını içerebilir.

İçeriden gelen tehditlerin tespiti ve önlenmesi aynı zamanda potansiyel içeriden gelen tehditleri gösteren anormal davranışları ve kalıpları belirlemek için makine öğrenimi, yapay zeka ve anlamsal analiz dahil olmak üzere ileri teknolojilerin kullanımını da içermektedir. İçeriden gelen tehditleri tespit etmek ve önlemek için kullanıcı davranışı analitiği, veri kaybı önleme sistemleri ve ayrıcalıklı erişim yönetimi çözümleri gibi teknolojilerden yararlanılmaktadır (Gheyas ve Abdellah, 2016).

2.2.10.13 Gelişmiş kalıcı tehditler

Gelişmiş Kalıcı Tehdit (APT), gizli, kalıcı ve iyi finanse edilmiş doğasıyla karakterize edilen karmaşık ve hedefe yönelik bir siber saldırı biçimidir. APT'ler,

devlet destekli gruplar veya organize siber suçlular gibi yüksek vasıflı ve becerikli tehdit aktörleri tarafından, devlet kurumları, kritik altyapılar ve büyük işletmeler de dahil olmak üzere belirli yüksek değerli hedeflerin bilgi sistemlerine sızmak ve bu sistemleri tehlikeye atmak amacıyla düzenlenir.

APT'ler uzun süreler boyunca tespit edilmeden kalacak şekilde tasarlanmıştır ve tehdit aktörlerinin tespit edilmeden casusluk yapmasına, hassas verileri sızdırmasına veya operasyonları aksatmasına sebep olabilir (Tizio vd., 2023). APT'lerin çalışma şekli, tipik olarak keşif, ilk etkileşim, dayanak oluşturma, yanal hareket, ayrıcalık yükseltme ve veri sızmasını içeren çok aşamalı bir saldırı yaşam döngüsünü içermektedir.

APT'ler, geleneksel güvenlik kontrollerini atlamak ve hedeflenen ağlara kalıcı erişim sağlamak için genellikle sıfır gün açıkları, özel kötü amaçlı yazılımlar ve sosyal mühendislik gibi gelişmiş tekniklerden yararlanır. Gelişmiş kaçınma taktiklerinin kullanılması ve savunma önlemlerine uyum sağlama yeteneği, APT'leri siber güvenlik ortamında zorlu ve kalıcı bir tehdit haline getirmektedir (Nafees vs., 2023).

APT tehditlerini ve etkilerini azaltmak için, tehdit istihbaratını, sürekli izlemeyi ve olaylara müdahale yeteneklerini kapsayan kapsamlı ve proaktif bir güvenlik duruşu sergilemeye bağlıdır. Kuruluşların, APT etkinliklerini tespit etmek ve bunlara yanıt vermek için ağ bölümlendirmesi, uç nokta algılama ve yanıt (EDR) ve kullanıcı davranışı analitiği gibi sağlam güvenlik kontrollerini uygulaması gerekir.

APT'lerin tespiti ve ilişkilendirilmesi genellikle APT faaliyetlerini tanımlamak ve ilişkilendirmek için makine öğrenimi, tehdit avcılığı ve adli analiz dahil olmak üzere gelişmiş güvenlik teknolojilerinin kullanımını içerir. Ayrıca, kamu ve özel sektör arasındaki iş birliği, bilgi paylaşımı ve uluslararası işbirliği, ulusötesi ve jeopolitik sonuçları göz önüne alındığında, APT'lerle mücadelede önemli bir rol oynamaktadır. APT'lerin kalıcı ve gelişen doğasına karşı etkili bir şekilde savunma yapmak için proaktif ve işbirlikçi bir yaklaşım esastır (Chu vd., 2019).

2.2.10.14 Mantık bombası

Mantık bombası, belirli bir koşul gerçekleştiğinde veya belirli bir zaman diliminde otomatik olarak harekete geçen kötü niyetli bir yazılım parçasıdır. Genellikle zararlı kodların, sistemin normale dönecek veya belirli bir kullanıcı

eylemini gerçekleştirecek bir zamana kadar gizli kalması sağlanır. Mantık bombalarının en büyük tehlikesi, kendilerini gizli bir şekilde kuluçka döneminde saklayabilmeleridir; bu süreçte, sistem üzerindeki herhangi bir belirgin anormallik yaratmazlar ve güvenlik yazılımlarından kaçabilirler. Ancak, kuluçka döneminin sona ermesiyle birlikte, önceden belirlenmiş koşul veya zaman geldiğinde, mantık bombası aktif hale gelir ve sistem üzerinde büyük çaplı zararlara neden olabilir.

Teknik olarak, mantık bombaları genellikle programlama dillerinde yazılmıştır ve genellikle kötü niyetli bir yazılım parçası olarak tasarlanır. Bu tür kodlar, belirli olaylara yanıt olarak çalışacak şekilde tasarlanabilir. Örneğin, bir mantık bombası, bilgisayar sisteminin belirli bir tarihi geçmesini, belirli bir kullanıcı eylemini (örneğin, bir dosyanın silinmesini) veya belirli bir süre boyunca belirli bir işlem yapılmamasını bekleyebilir (Keleştemur, 2015).

Bir mantık bombasının çalışması sırasında, bu tür kötü amaçlı yazılımlar, genellikle bir zamanlayıcı veya koşul denetleyicisi olarak işlev görebilir. Örneğin, bir mantık bombası, bir sistemin belirli bir tarihte veya belirli bir kullanıcı komutuyla aktif hale gelecek şekilde programlanmış olabilir. Kuluçka döneminde, mantık bombası, kötü niyetli kodun çalışmasını veya sistem kaynaklarını tüketen arka planda sessizce çalışabilir. Mantık bombalarının bazıları, veri yedekleme sistemlerini hedef alarak kritik verileri silme, dosyaları şifreleme veya sistem performansını ciddi şekilde düşürme gibi eylemler gerçekleştirebilir. Bunlar genellikle veri kaybına veya sistemin işlevselliğinin kaybına neden olabilir.

Güvenlik açısından, mantık bombalarının tespit edilmesi zor olabilir çünkü bunlar genellikle görünür bir zarara neden olmadan uzun süre gizli kalabilirler. Bu yüzden, güvenlik uzmanları, düzenli sistem denetimleri, güncellenmiş antivirüs yazılımları ve güvenlik yamaları ile mantık bombası ve diğer kötü amaçlı yazılım türlerine karşı proaktif önlemler almalıdır. Ayrıca, yazılım geliştiricileri ve sistem yöneticileri, potansiyel güvenlik açıklarını kapatmak ve kötü niyetli kodların sistemlere girmesini engellemek için dikkatli olmalıdır.

2.2.11 Siber riskler ve siber güvenlik

Siber güvenlik, bir kullanıcının veya bir işletmenin dijital varlıklarını siber tehditlerden korumak amacıyla tasarlanmış kapsamlı bir araçlar, yöntemler ve stratejiler dizisidir. Bu disiplin, sadece teknik çözümleri değil, aynı zamanda

organizasyonel politikaları, eğitim programlarını, risk yönetimi yaklaşımlarını ve güvenlik teminatlarını da içerir. Siber güvenlik, genellikle çeşitli teknolojik ve organizasyonel bileşenlerin bir arada kullanılmasıyla sağlanır, böylece dijital varlıkların gizliliği, bütünlüğü ve erişilebilirliği korunur (Keleştemur, 2015).

Teknik olarak, siber güvenlik, şifreleme yöntemleri, güvenlik duvarları, saldırı tespit sistemleri, saldırı önleme sistemleri, antivirüs yazılımları ve güvenli ağ protokollerini içerir. Şifreleme, verilerin yetkisiz erişime karşı korunmasını sağlarken, güvenlik duvarları ve IDS/IPS sistemleri, ağ üzerinde gerçekleşen anormal aktiviteleri tespit edip engelleyebilir. Antivirüs yazılımları, zararlı yazılımları tespit etmek ve etkisiz hale getirmek için kullanılır. Ayrıca, siber güvenlik, erişim kontrol sistemleri, kimlik doğrulama ve yetkilendirme mekanizmalarını da kapsar; bu sistemler, kullanıcıların ve sistemlerin sadece yetkilendirilmiş erişimlere sahip olmasını sağlar.

Siber güvenlik ayrıca, bir işletmenin siber tehditlere karşı savunma kapasitesini artırmak için sürekli izleme ve güncellemeyi içerir. Güvenlik açıklarını kapatmak için yazılım güncellemeleri ve yamaları düzenli olarak uygulanmalıdır. Ayrıca, güvenlik olaylarının anında tespit edilmesi ve yanıtlanması için olay yanıt ekipleri ve prosedürleri de kurulmalıdır.

Siber riskler, dijital sistemleri, ağları ve verileri etkileyebilecek çok çeşitli potansiyel tehditleri ve güvenlik açıklarını kapsamaktadır. Bu riskler, veri ihlalleri, siber saldırılar ve sistem açıkları dahil olmak üzere çeşitli şekillerde ortaya çıkabilir ve kuruluşlar, kritik altyapılar ve bireyler için önemli zorluklar oluşturabilir. Siber risklerin gelişen doğası, onları siber güvenlik alanında odak noktası haline getirmiş, etkilerini azaltmak ve potansiyel tehditlere karşı koruma sağlamak için proaktif önlemler alınmasını gerekli kılmıştır (Falco vd., 2019).

Siber risklerin yapısı karmaşık ve çok yönlü olup, dijital sistemlere ve bilgi varlıklarına yönelik geniş bir potansiyel tehdit yelpazesini kapsamaktadır. Bu riskler, gelişmiş kalıcı tehditler (APT'ler) gibi hedefli siber saldırılardan kimlik avı dolandırıcılıkları, kötü amaçlı yazılım bulaşmaları ve fidye yazılımı saldırıları gibi daha yaygın güvenlik açıklarına kadar değişebilir.

Siber riskleri yönetmek, tehdit istihbaratını, risk değerlendirmesini ve güçlü güvenlik kontrollerinin uygulanmasını kapsayan kapsamlı ve proaktif bir yaklaşım

gerektirir. İşletmelerin, siber riskleri etkili bir şekilde azaltmak için düzenli güvenlik değerlendirmelerini, güvenlik açığı yönetimini ve olay müdahale yeteneklerini içeren bütünsel bir siber güvenlik stratejisini benimsemeleri gerekmektedir.

Siber risk yönetiminin genel kurumsal risk yönetimi çerçevelerine entegrasyonu, potansiyel tehditlere yönelik koordineli ve proaktif bir yaklaşım sağlamak için önemlidir (Orlando, 2021). Siber risklerin gelişen doğası, potansiyel tehditleri etkili bir şekilde ele almak için disiplinler arası işbirliği ve bilgi paylaşımı ihtiyacını da vurgulamıştır.

Siber risk araştırmaları, siber risklere ilişkin kapsamlı bir anlayış kazanmak ve etkili azaltma stratejileri geliştirmek için disiplinler arası işbirliğinin önemini vurgulayan disiplin engelleri nedeniyle sekteye uğramaktadır. Kuruluşlar, hukuk, bilgisayar bilimi ve işletme gibi çeşitli disiplinler arasındaki işbirliğini teşvik ederek, siber risklerin karmaşık ve gelişen doğasını ele alma yeteneklerini geliştirebilirler.

Dijital teknolojiye ve nesnelerin internetine (IoT) artan bağımlılık, özellikle kritik altyapı ve tedarik zinciri güvenliği bağlamında siber risklerin yeni boyutlarını da beraberinde getirmiştir. IoT cihazlarının birbirine bağlı yapısı ve dijital teknolojilerin kritik altyapı sistemlerine entegrasyonu, potansiyel siber risklere yönelik saldırı yüzeyini genişletmiştir. Bu sebeplerden dolayı, IoT ile ilgili siber risklerin ortaya çıkardığı benzersiz zorlukların üstesinden gelmek için uzmanlaşmış siber risk yönetimi çerçevelerine ve stratejilerine artan bir ihtiyaç doğmaktadır.

2.2.12 Siber risk yönetimi

Siber risk yönetimi, modern işletmelerin dijital varlıklarını ve operasyonlarını, potansiyel tehditlerden ve güvenlik açıklarından koruma stratejilerinin kritik bir bileşenidir. Veri ihlalleri, siber saldırılar ve sistem açıkları dahil olmak üzere siber risklerin gelişen doğası, bu risklerin yönetilmesinde proaktif ve kapsamlı bir yaklaşımı gerektirmektedir. Siber risk yönetimi, dijital sistemlere ve bilgi varlıklarına yönelik potansiyel tehditlerin tanımlanmasını, değerlendirilmesini ve azaltılmasını içerir.

İşletmelerin, sağlam güvenlik kontrolleri, tehdit istihbaratı ve olay müdahale yeteneklerini benimsemesini gerektirir (Kure vd., 2022). Siber risk yönetimi, potansiyel tehditleri etkili bir şekilde ele almak için siber risk değerlendirmesinde gelecekteki gelişmeleri içeren ileriye dönük bir yaklaşıma ihtiyaç duyar.

Gelişmiş ve kapsamlı bir siber güvenlik risk yönetimi çerçevesi, hızla değişen tehdit ortamına ve gelişen karmaşık siber saldırıların varlığına yanıt vermede önemli bir rol oynamaktadır. Bu çerçeve, potansiyel tehditleri azaltmak için risk değerlendirmesini, risk tahminini ve güvenlik kontrollerinin uygulanmasını kapsamaktadır. İşletmeler, siber güvenlik risk yönetimini genel risk yönetimi çerçevelerine entegre ederek, siber risklerin çok yönlü doğasını etkili bir şekilde ele alabilir ve potansiyel tehditlere karşı dayanıklılıklarını artırabilir.

Özellikle verilerin klasik istatistiksel modeller oluşturmak için yeterli olmadığı durumlarda, siber risk yönetiminde yapay zeka (AI) yöntemleri giderek yaygınlaşmaktadır. Bu yöntemler, potansiyel siber risklerin göstergesi olan anormal davranışların ve kalıpların belirlenmesinde önemli bir rol oynamakta ve böylece işletmelerin karmaşık siber tehditlere karşı savunmasını güçlendirmektedir (Giudici ve Raffinetti, 2021). Risk niceliği, siber risk yönetiminin önemli bir yönü haline gelmiştir; siber risk yönetimi teknikleri, finansal alanda yaygın olarak kullanılan risk niceliğine dayalı önlemleri giderek daha fazla içermektedir. Bu önlemler, işletmelere potansiyel kayıpları ölçmek ve siber risklerin etkisini değerlendirmek için bir araç sağlayarak geçmiş verilere ve öngörülen olaylara dayanarak bilinçli risk yönetimi kararları almalarına olanak tanımaktadır.

Siber risk yönetimi, işletmelerin siber saldırılardan kaynaklanan kayıpların dağıtımını sağlayan risk analizi modelleri ve vaka çalışmaları ile kritik altyapı koruması için de çok önemlidir. Bu dağıtımlar hem geçmiş verilere hem de beklenen olaylara dayalı risk yönetimi kararlarını destekleyerek, işletmelerin potansiyel tehditleri ve güvenlik açıklarını değerlendirmesine ve etkili risk azaltma stratejileri uygulamasına imkan tanımaktadır. Siber-fiziksel sistemlerin birbirine bağlı yapısı ve dijital teknolojilerin kritik altyapı sistemlerine entegrasyonu, potansiyel siber risklere yönelik saldırı yüzeyini genişletmiştir.

Günümüzde, siber-fiziksel sistemle ilgili siber risklerin ortaya çıkardığı benzersiz zorlukları ele almak için uzmanlaşmış siber risk yönetimi çerçevelerine ve stratejilerine artan bir ihtiyaç duyulmaktadır. Bu çerçeveler, kritik altyapı sistemlerini potansiyel tehditlerden korumak için potansiyel güvenlik açıklarının belirlenmesinde ve etkili risk azaltma stratejilerinin uygulanmasında önemli bir rol oynamaktadır (Radanliev ve diğerleri, 2021).

Uluslararası siber yönetişimin olmayışı, siber güvenlik politikalarının uygulanmasını engellemekte, özellikle ticari havacılıkta siber güvenlik risklerinin değerlendirilmesi ve yönetilmesine yönelik standartlar ve en iyi uygulamalar oluşturmak için küresel tabanlı bir ittifakı zorunlu kılmaktadır.

Risk yönetimini uygulamamanın sonuçları olarak, siber tehditlerin zayıf kontrolüne ve yönetimine yol açması ve bu da potansiyel tehditlerle mücadelede etkili siber risk yönetimi stratejilerinin öneminin artması beklenmektedir (Nobles vd., 2022). Siber risk yönetimi, potansiyel tehditleri ve güvenlik açıklarını etkili bir şekilde ele almak için proaktif ve kapsamlı bir yaklaşım gerektiren çok yönlü ve gelişen bir disiplindir.

2.2.13 Siber uzay ve siber güvenlik ortamı

Siber uzay, çeşitli akademik disiplinlerin dikkatini çeken çok yönlü bir alandır. Hem tehditleri hem de fırsatları sunduğu için ulusal güvenliğe etkileri olan sanal bir uzayı ifade etmektedir. Siber uzaydaki insan hareketlerinin ve bunun fiziksel uzayla olan ilişkisinin incelenmesi, ilginç ölçeklendirme ve korelasyon modellerini ortaya çıkarmış ve bu iki alanın birbirine bağlılığına ışık tutmuştur (Zhao vd., 2014). Bilgi teknolojileri ve uzay arasındaki etkileşim eleştirel bir şekilde analiz edilmiş ve aralarındaki ilişkilerin siber uzay bağlamında kavramsallaştırılması ihtiyacı vurgulanmıştır (Graham, 2004).

Ayrıca, siber uzayın sosyal etkileşim ve refah üzerindeki etkisi, özellikle çevrimiçi sosyal etkileşimdeki bedenden arınma ve bunun sosyal destek ve psikososyal refah üzerindeki etkileri açısından araştırılmıştır (Kang, 2007). Siber uzayın sosyal, bilgi ve coğrafi katmanları içeren birbirine bağlı ağlar olarak kavramsallaştırılması, bu sanal alanın çok yönlü doğasını vurgulamaktadır (Asquith ve Morgan, 2020).

Siber güvenlik ortamı, çok çeşitli birbirine bağlı faktörleri kapsayan karmaşık ve hızla gelişen bir alandır. Teknolojik gelişmelerin, düzenleyici çerçevelerin, insan faktörlerinin ve sürekli değişen tehdit ortamının etkileşimini içerir. Ayrıca, siber güvenlik ortamı, siber güvenlik uzmanlarına yönelik artan talep, siber güvenliğe yönelik entegre bir yaklaşıma duyulan ihtiyaç, otonom araçlar ve IoT gibi yeni çıkan teknolojilerin ortaya çıkardığı zorluklarla şekillenmektedir (Singh ve diğerleri, 2023).

İşletmeler, siber güvenlik ortamının haritalandırılmasında ve yönetilmesinde önemli bir rol oynamaktadır. İster uluslararası ister ulusal organlar tarafından görevlendirilsin, siber güvenlik ortamındaki resmi kuruluşlar, siber güvenliğin kurumsal manzarasının şekillendirilmesine katkıda bulunmaktadır (Kuerbis ve Badiei, 2017).

Siber güvenlik standartlarının ve düzenlemelerinin hükümetler ve düzenleyici kurumlar tarafından geliştirilmesi ve uygulanması, temel IoT güvenlik gereksinimlerini ve siber güvenlik sertifikasyon planlarını etkileyerek siber güvenlik ortamını önemli ölçüde etkilemektedir. İnsan faktörü, siber güvenlik ortamının bir diğer kritik yönüdür. Bireylerin siber güvenliğe ilişkin algıları, siber güvenlik mesleğindeki stres ve kadınların siber güvenlik alanında temsili, siber güvenliğin insani boyutunun şekillenmesine katkıda bulunmaktadır (Ramlo ve Nicholas, 2021).

Çok disiplinli siber güvenlik ekiplerine duyulan ihtiyaç, siber güvenlik ortamındaki çok yönlü zorlukların üstesinden gelmede bilgi işlem, yöneylem araştırması, yapay zeka ve psikoloji dahil olmak üzere çeşitli uzmanlıkların önemi artmaktadır. Gelişen tehdit ortamı, siber güvenlik alanında merkezi bir endişe kaynağıdır. Siber suçlular tekniklerini sürekli geliştirerek hem işletmeleri hem de bireyleri etkileyen etkili saldırılara yol açmaktadır. Bu saldırılar, siber güvenliğe dinamik ve uyarlanabilir bir yaklaşım gerektirmektedir. Ayrıca gelecekteki siber saldırıların ve ilgili siber güvenlik önlemlerinin tahmini, gelişen tehdit ortamını anlamak ve buna hazırlanmak açısından oldukça önemlidir (AL-Hawamleh, 2023).

2.2.14 Siber güvenlik önlemleri

Siber güvenlik önlemleri, çeşitli alanların siber tehditlere karşı korunmasında temel bileşenlerdir. Denizcilik sektöründe kullanılan endüstriyel kontrol sistemleri (ICS) bağlamında, bu sistemlerin tehlikeye atılması çok büyük fiziksel hasara ve insan hayatı için tehlikelere yol açabilmektedir (Bhamare vd., 2020). Endüstriyel yönetimde IoT, endüstriyel sistemleri korumak için etkili siber güvenlik önlemlerine olan ihtiyacı vurgulayan güvenlik kaygıları sunmaktadır (Raimundo ve Rosário, 2022).

Otonom gemilerin ortaya çıkışı, bu sistemlerin zeka, karmaşıklık ve enerji verimliliği yönlerini ele alacak kapsamlı karşı önlemleri gerektirmektedir (Algarni ve Thayananthan, 2023). Ayrıca, siber güvenlik önlemlerinde insan faktörü kritik bir

hususdur. Bireylerin siber güvenliğe ilişkin algılarını değerlendirmek, insan davranışlarını ve güvenliğe yönelik tutumları açıklayan etkili karşı önlemlerin geliştirilmesinde önemlidir (Ramlo ve Nicholas, 2021). Küresel bir ağdan oluşan siber uzayda ortaya çıkan kablosuz ağ sistemlerinin ve siber güvenliğin etkisi, kablosuz ağlarda artan tehditlere karşı proaktif siber güvenlik önlemlerinin alınması da büyük ölçüde önem arz etmektedir.

Siber güvenlik önlemleri, çeşitli alanlarda gelişen siber tehditlerin ele alınmasında önemli bir rol oynamaktadır. Denizcilik sektöründen gemilere, işletmelerin bilişim alt yapılarından endüstriyel kontrol sistemlerine, IoT'ye, otonom gemilere ve köprü üstü sistemleri ile makine üretimine kadar etkili siber güvenlik önlemlerinin geliştirilmesi ve uygulanması, risklerin azaltılması, kritik sistemlerin ve altyapının dayanıklılığının sağlanması açısından önemlidir.

2.2.15 Kurumsal siber güvenlik önlemleri

Kurumsal siber güvenlik önlemleri, işletmelerin dijital varlıklarının ve operasyonlarının korunmasında kritik öneme sahiptir. Siber tehditlerin artan sıklığı ve karmaşıklığı, hassas bilgilerin korunması, operasyonel sürekliliğin ve paydaşların güveninin sürdürülmesi için sağlam önlemlerin alınmasını gerektirmektedir. Siber güvenlik önlemleri; riskleri azaltmayı, güvenlik olaylarını tespit edip bunlara yanıt vermeyi ve işletmelere ait sistem ve ağların dayanıklılığını sağlamayı amaçlayan çok çeşitli stratejileri, teknolojileri ve uygulamaları kapsar.

Gelişmekte olan ülkelerdeki küçük ve orta ölçekli işletmeler (KOBİ'ler), kendilerine özgü ihtiyaç ve kısıtlamalara yönelik özel siber güvenlik önlemleri gerektiren farklı siber güvenlik sorunlarıyla karşı karşıyadır. KOBİ'lerdeki siber güvenlik uygulamalarının araştırılması, kaynak sınırlamaları ve teknolojik yetenekler dikkate alınırken, siber riskleri etkili bir şekilde azaltabilecek uygun maliyetli ve ölçeklenebilir önlemlerin önemi ortaya çıkmaktadır (Kabanda vd., 2018).

Kritik altyapı koruması alanında siber güvenlik önlemleri, enerji, su ve ulaşım sistemleri gibi temel hizmetlerin güvenliğinin ve dayanıklılığının sağlanmasında önemli bir rol oynamaktadır. Kritik altyapıya yönelik bir siber güvenlik yönetim modeli, kritik altyapıyı siber tehditlerden korumak için organizasyonel, teknolojik, yasal ve stratejik yönleri kapsayan kapsamlı önlemlere ihtiyaç duymaktadır (Tvaronavičienė vd, 2021).

Ticari işletmeler için sürdürülebilir siber güvenliğe ulaşmada yönetişimin rolü, entegre bir yaklaşım gerektirmektedir. Ticari işletmelerdeki etkili siber güvenlik önlemleri, yetkisiz erişime, veri ihlallerine ve endüstriyel casusluğa karşı koruma sağlamak için yönetişim mekanizmalarının siber güvenlik hedefleriyle stratejik olarak hizalanmasını gerektirir (Alashi ve Badi, 2020).

İşletme personeli bireysel olarak önemli siber güvenlik riskleri oluşturabileceğinden, işletmelerde siber güvenlik önlemlerinin benimsenmesi ve insan faktörünün de ele alınmasını gerektirir. Bireylerin siber güvenliğe ilişkin algılarını değerlendirmek, insan davranışlarını ve güvenliğe yönelik tutumlarını hesaba katan, eğitim ihtiyacını, davranış değişikliklerini ve güvenlik ihlali potansiyelini vurgulayan etkili karşı önlemlerin geliştirilmesi açısından oldukça önemlidir (Ramlo ve Nicholas, 2021).

2.3 Denizcilik ve Uluslararası Ticaret

Denizcilik, bölgesel istihdam pazarlarını sağlayan, küresel ekonomiyi önemli ölçüde paylaşan çok yönlü bir sektördür. Denizcilik, gemi inşası, liman operasyonları, deniz balıkçılığı, açık deniz petrol ve gazı, deniz savunması ve kıyı eğlence faaliyetleri dahil olmak üzere çeşitli endüstrileri kapsamaktadır (To ve Lee, 2018). Denizcilik sektörü, ekonomik büyüme ve küresel ticaret etkileri ile ulaşım güvenliği ve güvenliği ile bağlantılıdır. Endüstri 4.0, denizcilik sektöründe genişleyen dijitalleşmesini ve otomasyonunu gibi sunduğu yeteneklerle birlikte önem kazanmıştır.

Denizcilik sektöründeki simülasyon eğitimi ve denizcilik düzenlemeleri eğitimi için yapay zeka sohbet robotlarının aracılığıyla insani ve kurumsal hataları azaltma çabaları, ekonomik güvenlik ve verimliliğe olan bağlılığının sınıflandırılması daha da önemli hale gelmiştir (Barić vd., 2018). Denizcilik kümelenmelerinin ekonomik önemi ve istihdam ile GSYİH üzerinde doğrudan ve dolaylı etkileri, sektörün toplumdaki hayati rolü oldukça büyüktür (Viederytė, 2021).

Deniz ticareti, küresel ekonomide önemli bir rol oynamakta ve uluslararası ticaretin temel taşı olarak hizmet vermektedir. Deniz ticaretinin önemi, tüm küresel ticaret faaliyetlerinin önemli bir bölümünü temsil eden küresel ithalat-ihracat ticaretine önemli katkısıyla vurgulanmaktadır. Bu nedenle, denizcilik sektörüne

yönelik siber saldırılara ve bunlara karşı alınması gereken önlemlere ilişkin standartlar büyük önem taşımaktadır.

2.3.1 Deniz taşımacılığının ekonomik etkisi

Deniz taşımacılığının ekonomik etkileri oldukça büyüktür; sadece ticareti desteklemekle kalmaz, aynı zamanda ekonomik büyüme oranlarını da etkiler. Konuyla ilgili yapılan, taşımacılık maliyetlerinin iki katına çıkmasının ekonomik büyüme oranlarının yarıya inmesine yol açabileceğini, özellikle daha yüksek iç taşımacılık maliyetleriyle karşı karşıya olan karayla çevrili ülkeleri etkileyebileceğini göstermektedir (Park vd., 2019). Dahası, deniz taşımacılığı, daha hızlı olmasına rağmen önemli ölçüde daha pahalı olan hava taşımacılığının kapasitesini çok aşan kapasitesiyle emtia nakliyesinin lojistiğinin ayrılmaz bir parçasıdır.

Çizelge 2.5: Deniz Taşımacılığı Maliyetlerindeki Artışın Küresel Ekonomiye Etkisi

Ülke Türü	Nakliye Maliyeti Artışı (%)	GSYİH Büyüme Azalması (%)	Etkilenen Sektörler	Açıklama
Kıyı Ülkeleri	%10	%0.5	İhracat, İthalat, Sanayi, Tarım	Kıyı ülkeleri, deniz taşımacılığına doğrudan erişim sayesinde nakliye maliyetlerinden daha az etkilenir.
Karayla Çevrili Ülkeler	%10	%1.5	Tarım, Madencilik, Sanayi	Karayla çevrili ülkeler, deniz limanlarına erişim sağlamak için ek kara taşımacılığı maliyetlerine katlanır.
Gelişmekte Olan Ülkeler	%15	%2.0	Tarım, Tekstil, İmalat	Bu ülkelerde düşük kar marjlı sektörler, artan nakliye maliyetlerinden daha fazla etkilenir.
Gelişmiş Ülkeler	%5	%0.2	Yüksek Teknoloji, Otomotiv, Kimya	Gelişmiş ülkeler, daha fazla çeşitlendirilen ekonomileri ve güçlü altyapıları ile nakliye maliyet artışlarını daha iyi absorbe eder.

Deniz taşımacılığından elde edilen ekonomik faydalar, salt maliyet tasarruflarının ötesine geçer; ayrıca artan ticaret akışları yoluyla ekonomik büyümenin teşvik edilmesini de içerir. Deniz taşımacılığı ile ekonomik büyüme arasındaki etkileşim, nakliye rotalarının verimliliğini ve ulusların genel ekonomik performansını birbirine bağlayan çeşitli çalışmalarda açıkça görülmektedir

(Alekseievska, 2023). Doğrudan ekonomik etkilere ek olarak, deniz taşımacılığının çevresel sürdürülebilirlik için de önemli etkileri bulunmaktadır.

Denizcilik sektörü, çevresel ayak izini azaltmak için daha yeşil teknolojiler ve uygulamalar benimseme konusunda artan bir baskı altındadır. Daha temiz yakıtların ve yenilikçi pervane/itme sistemlerinin tanıtımı, gemilerden kaynaklanan emisyonları azaltmayı amaçlayan katı düzenlemelere bir yanıt olarak nitelendirilmektedir. Bu değişim, yalnızca çevresel endişeleri ele almakla kalmaz, aynı zamanda yakıt tüketimi ve düzenleyici standartlara uyumla ilişkili operasyonel maliyetleri azaltma ekonomik zorunluluğuyla da uyumludur (Alzayedi vd., 2022).

Deniz taşımacılığının ekonomik manzarası, Süveyş Kanalı gibi geleneksel nakliye yollarına kıyasla seyahat mesafesinde ve süresinde önemli azalmalar sunan Kuzey Denizi Rotası (NSR) gibi ortaya çıkan rotalardan da etkilenmektedir (Min vd., 2022). Bu yaklaşım, yalnızca Arktik nakliyesinin ekonomik uygulanabilirliğini artırmakla kalmamakta, aynı zamanda küresel ısınmanın seyir modellerini değiştirmesiyle ticaret için yeni fırsatlar da sunmaktadır (Zhao ve Hu, 2016). Bu tür rotaları kullanmanın potansiyel ekonomik faydaları önemlidir; daha düşük nakliye maliyetlerine ve azaltılmış emisyonlara yol açabilir ve çevresel hususları ekonomik planlamaya daha fazla entegre edebilir (Min vd., 2022).

2.3.2 Gemi güvenliğini yöneten temel kurallar ve standartlar

Gemilerin, mürettebatın ve kargonun emniyetini ve güvenliğini sağlamak, küresel tedarik zincirlerinin bütünlüğünü ve deniz ortamını korumak için gemi güvenliğini yöneten temel kurallar ve stantlara uyum oldukça önemlidir. Bu zorlukların üstesinden gelmek için, gemi güvenliğinin çeşitli yönlerini yöneten kapsamlı bir uluslararası kurallar ve standartlar çerçevesi oluşturulmuştur.

Uluslararası Güvenlik Yönetimi (ISM) Kodu, Uluslararası Gemi ve Liman Tesisi Güvenliği (ISPS) Kodu ve Denizde Can Güvenliği Uluslararası Sözleşmesi (SOLAS) gibi düzenlemeler, riskleri yönetmek, kazaları önlemek ve güvenlik tehditlerine yanıt vermek için yapılandırılmış çeşitli yönergeler sağlamaktadır. Bu standartlara uymak, gemilerin uluslararası sularda güvenli ve emniyetli bir şekilde işletilmesini sağlamak açısından önem arz etmektedir.

2.3.2.1 Uluslararası güvenlik yönetimi (ISM) kodu

IMO tarafından 1993 yılında kabul edilen ve 2002 yılında uygulamaya konulan Uluslararası Güvenlik Yönetimi (ISM) Kodu, deniz güvenliğini ve çevre korumasını geliştirmeyi amaçlayan temel bir düzenleyici çerçeveyi temsil etmektedir. ISM Kodu, nakliye şirketlerinin gemilerin güvenli bir şekilde işletilmesini ve deniz kirliliğinin önlenmesini sağlamak için bir Güvenlik Yönetim Sistemi (SMS) kurmasını zorunlu kılmaktadır.

Bu gereklilik, denizcilik sektöründe kendi kendini düzenlemeye doğru bir kaymayı yansıtır ve gemi yöneticilerini işyeri sağlığı ve güvenliğinden sorumlu olmaya zorlamaktadır. ISM Kodunun uygulanması, denizcilik sektöründe bir güvenlik kültürünün teşvik edilmesinde etkili olmuş ve sistematik güvenlik yönetimi uygulamalarının önemini vurgulamıştır (Batalden ve Sydnes, 2013).

ISM Kodunun temel hedeflerinden biri, denizcilik şirketleri arasında proaktif bir güvenlik kültürü oluşturmaktır. Bu kültür, yalnızca güvenlik düzenlemelerine uyumu değil, aynı zamanda etkili eğitim, risk değerlendirmesi ve olay raporlaması yoluyla güvenlik uygulamalarının sürekli iyileştirilmesini de içermektedir. Kod, şirketleri geçmiş olaylardan ders almaya teşvik ederek gelecekteki kazaların olasılığını azaltır.

İyi niyetli çerçevesine rağmen, ISM Kodu etkinliği konusunda eleştirilerle karşı karşıya kalmıştır. Çalışmalar, Kodun güvenlik yönetimi uygulamalarında iyileştirmelere yol açarken, bazen operasyonel verimliliği engelleyebilen artan bürokrasiye de yol açtığını göstermiştir (Demirci ve Çiçek, 2022).

Teknolojik gelişmeler de ISM Kodunun uygulanmasının evriminde önemli bir rol oynamıştır. Kağıt tabanlı sistemlerden dijital platformlara geçiş, güvenlik yönetimi süreçlerini basitleştirmiş, veri toplama ve analiz yeteneklerini geliştirmiştir. Bu değişim yalnızca ISM Koduna uyumu iyileştirmekle kalmamakta, aynı zamanda denizcilik sektöründe yüksek güvenlik standartlarının sürdürülmesi için kritik öneme sahip olan güvenlik uygulamalarının ve olay raporlamasının gerçek zamanlı izlenmesini de kolaylaştırmaktadır. Ancak, teknolojiye bağımlılık, güvenlik uygulamalarının kurumsal kültüre etkili bir şekilde entegre edilmesini sağlamak için insan gözetimi ve katılımına duyulan ihtiyaçla dengelenmelidir (Kececi, 2021).

2.3.2.2 Uluslararası güvenlik yönetimi (ISM) kodu

Uluslararası Gemi ve Liman Tesisi Güvenliği (ISPS) Kodu, 11 Eylül 2001 terörist saldırılarının ardından artan güvenlik endişelerine yanıt olarak geliştirilmiştir. IMO, özellikle deniz taşımacılığı sistemlerinin güvenlik açıklarını ele almak için Denizde Can Güvenliği (SOLAS) Sözleşmesi'ndeki değişikliklerin bir parçası olarak ISPS Kodunu benimsemiştir.

Kod, güvenlik risklerini değerlendirmek ve yönetmek için kapsamlı bir çerçeve oluşturarak gemilerin ve liman tesislerinin güvenliğini artırmayı amaçlamaktadır. Uluslararası ticaret ve liman tesislerinde faaliyet gösteren tüm gemilerin, Gemi Güvenlik Planları (SSP'ler) ve Liman Tesisi Güvenlik Planları (PFSP'ler) geliştirilmesi de dahil olmak üzere belirli güvenlik önlemleri uygulamasını zorunlu kılmaktadır.

ISPS Kodunun temel bileşenlerinden biri, potansiyel güvenlik tehditlerini ve güvenlik açıklarını belirlemek için risk değerlendirmeleri gereksinimidir. Bu süreç, halihazırda yürürlükte olan güvenlik önlemlerinin değerlendirilmesini ve belirlenen riskleri azaltmak için gerekli iyileştirmelerin belirlenmesini içerir. Kod, güvenlik protokollerine uyumu sağlamak için sürekli izleme ve düzenli denetimlerin önemini vurgulamaktadır.

ISPS Kodu, azami dikkati ve hazırlık kültürünü teşvik ederek denizcilik sektöründe proaktif bir güvenlik ortamı yaratmayı amaçlamaktadır (Hasanov ve Alsulaiman). Bu önlemlerin uygulanması, deniz güvenliği ve emniyeti için önemli tehditler oluşturan korsanlık, kaçakçılık ve terörizm gibi olayların önlenmesi açısından oldukça önemlidir.

ISPS Kodu ayrıca hükümet yetkilileri, nakliye şirketleri ve liman tesisi operatörleri dahil olmak üzere çeşitli paydaşlar arasında iş birliğine olan ihtiyacı vurgulamaktadır. Güvenlik önlemlerinin başarılı bir şekilde uygulanması ve güvenlik olaylarına yanıt verilmesi için etkili iletişim ve koordinasyon esastır. Kod, deniz operasyonlarında yer alan personelin hazırlığını artırmak için güvenlik komitelerinin kurulmasını ve düzenli eğitim tatbikatlarını teşvik etmektedir.

Kapsamlı çerçevesine rağmen, ISPS Kodu uygulanmasında zorluklarla karşılaşılmıştır. Farklı ülkeler ve limanlar arasında uyumluluk seviyelerindeki değişkenlik, Kodun genel etkinliği konusunda endişelere yol açmıştır. Bazı

çalışmalar, büyük limanların güvenliği artırmada önemli ilerlemeler kaydetmiş olsa da daha küçük ve daha az kaynaklı tesislerin ISPS Kodu tarafından belirlenen gereklilikleri karşılamakta zorlanabileceğini göstermiştir (Ibrahim, 2024). Siber tehditler ve teknolojik güvenlik açıkları gelişmeye devam ettikçe, yeni teknolojilerin ve uygulamaların mevcut güvenlik çerçevelerine entegre edilmesi, iyileştirme için kritik bir alan olmaya devam etmektedir.

2.3.2.3 Denizde can güvenliği uluslararası sözleşmesi (SOLAS)

Denizde Can Güvenliği Uluslararası Sözleşmesi (SOLAS), gemilerin ve mürettebatlarının güvenliğini sağlamayı amaçlayan en önemli denizcilik anlaşmalarından biridir. İlk olarak 1914 yılında Titanic felaketine yanıt olarak kabul edilen SOLAS, denizcilik operasyonlarındaki gelişen güvenlik endişelerini ele almak için çeşitli değişiklikler ve güncellemeler geçirmiştir.

Sözleşme, gemilerin inşası, ekipmanı ve işletimi için asgari güvenlik standartlarını belirleyerek, deniz güvenliği için kapsamlı bir çerçeve oluşturmaktadır. Uluslararası Denizcilik Örgütü, SOLAS'ın uygulanmasını denetlemekte ve üye devletlerin hükümlerine uymasını ve güvenlik önlemlerini sürekli olarak iyileştirmesini sağlamaktadır.

SOLAS'ın temel özelliklerinden biri, gemi tasarımı ve inşasıyla ilgili katı düzenlemeler yoluyla denizde can güvenliğine odaklanmasıdır. Sözleşme, acil durumlarda yolcuları ve mürettebatı korumak için cankurtaran botları, can yelekleri ve yangın söndürme sistemleri gibi temel güvenlik ekipmanlarıyla donatılmasını zorunlu kılmaktadır. Ayrıca SOLAS, gemi operatörlerinin güvenlik standartlarına uyumu sağlamak için düzenli güvenlik tatbikatları, risk değerlendirmeleri ve bakım kontrolleri yapılmasını zorunlu kılan güvenlik yönetim sistemleri için gereklilikleri ana hatlarıyla belirtmektedir. Güvenlik yönetimine yönelik bu proaktif yaklaşım, yıllar içinde deniz kazalarının ve ölümlerin sayısını önemli ölçüde azaltmıştır.

SOLAS, gemi güvenliğini ele almanın yanı sıra mürettebat eğitimi ve yeterliliğinin de önemini vurgulamaktadır. Sözleşme, mürettebat üyelerinin acil durum prosedürleri ve güvenlik ekipmanlarının kullanımı konusunda yeterli eğitim almasını şart koşmaktadır. İnsan faktörünü ele alan bu odaklanma, etkili güvenlik yönetiminin yalnızca teknolojiye ve ekipmana değil, aynı zamanda mürettebatın acil durumlarda hazırlığına ve tepkisine de bağlı olduğunu kabul etmektedir. Sürekli

mesleki gelişim ve eğitim programları, yüksek güvenlik standartlarını korumak ve mürettebat üyelerinin olası krizlerle başa çıkabilecek şekilde donatılmasını sağlamak için esastır.

SOLAS sözleşmesi ayrıca deniz operasyonlarının artan karmaşıklığı ve yeni teknolojilerin yükselişi gibi deniz güvenliğindeki ortaya çıkan zorlukları ele almak için de gelişmiştir. Son değişiklikler, yolcu gemilerinin güvenliğiyle ilgili düzenlemeler getirmiştir; bunlara denge, yangın güvenliği ve tahliye prosedürleri için geliştirilmiş gereklilikler de dahildir.

Bunlara ek olarak, sözleşme, giderek dijitalleşen bir ortamda modern gemilerin karşılaştığı güvenlik açıklarını kabul ederek siber güvenlikle ilgili hususları da dahil etmeye başlamıştır (Joseph ve Dalaklis, 2021). Bu güncellemeler, denizcilik sektörünün değişen koşullara uyum sağlama ve güvenlik önlemlerini sürekli olarak geliştirme konusundaki devam eden taahhüdünü yansıtmaktadır.

2.3.2.4 Denizcilik çalışma sözleşmesi (MLC)

Uluslararası Çalışma Örgütü (ILO) tarafından 2006 yılında kabul edilen Denizcilik Çalışma Sözleşmesi (MLC), denizciler için insan onuruna yakışır çalışma ve yaşam koşulları sağlamayı amaçlayan kapsamlı bir uluslararası yasal araçtır. Genellikle "Denizcilerin Hakları Bildirgesi" olarak anılan MLC, çok sayıda mevcut ILO sözleşmesini ve tavsiyesini tek bir çerçevede birleştirerek, istihdam sözleşmeleri, ücretler, çalışma saatleri, sağlık ve güvenlik ile konaklama standartları dahil olmak üzere denizcilik emeğinin çeşitli yönlerini ele almaktadır (Mantoju, 2021).

MLC'nin temel hedeflerinden biri, denizcilerin çalışma ve yaşam koşulları için asgari standartlar belirleyerek refahlarını artırmaktır. Bunlara yeterli konaklama, eğlence tesisleri ve tıbbi bakıma erişim için hükümler dahildir. MLC ayrıca denizcilerin adil ücretlere ilişkin haklarının ve onları sömürüden korumak için çok önemli olan şeffaf istihdam sözleşmelerinin gerekliliğinin önemini vurgulamaktadır. MLC, bu standartları belirleyerek gemi donatanları için eşit şartlar yaratmayı ve tüm denizcilerin milliyetlerine veya gemilerinin bayrak devletine bakılmaksızın, adil bir şekilde muamele görmesini sağlamayı amaçlamaktadır.

MLC'nin uygulanması denizcilerin çalışma koşullarında önemli iyileştirmelere yol açmıştır. Çalışmalar, sözleşmenin denizcilerin ruh sağlığı ve genel

refahı da dahil olmak üzere denizcilerin yaşamlarının çeşitli yönlerini olumlu yönde etkilediğini göstermiştir. Sözleşmenin mesleki güvenlik ve sağlığa odaklanması, nakliye şirketlerini mürettebatlarını işyeri tehlikelerinden korumak için daha iyi uygulamalar ve protokoller benimsemeye yöneltmiştir (Graham ve Walters, 2020).

Teknolojik gelişmeler kadar, MLC'nin de etkisiyle günümüzde çalışanlara refah bir alan ve çeşitli kullanım kolaylıkları sunan otonom gemiler inşa edilmektedir. Bu otonom gemiler, gemi personeli için bir nevi akıllı şehir olarak tanımlanabilecek bir yaşam mahali de sunmaktadır. Ancak bu teknolojik gemilerin, geleneksel gemilere oranla, siber saldırılara çok daha fazla maruz kaldığı ve yine çok daha fazla etkilendiği görülmektedir.

2.3.2.5 Güvenlik yönetim sistemlerinde deniz siber risk yönetimi

IMO, Haziran 2017'de denizcilik operasyonlarındaki siber risklerle ilgili artan endişeleri ele almak için MSC.428(98) ekini yayınlamıştır. Bu karar, denizcilik işletmelerinin güvenlik ve emniyete yönelik kapsamlı bir yaklaşımın parçası olarak siber risk yönetimini Güvenlik Yönetim Sistemlerine (SMS) entegre etme ihtiyacını vurgulamaktadır. IMO, siber risk yönetiminin mevcut SMS çerçevelerine dahil edilmesini zorunlu kılarak, denizcilik operasyonlarının siber tehditlere karşı dayanıklılığını artırmayı amaçlamaktadır.

MSC.428(98)'in temel yönlerinden biri, siber güvenlik risklerini yönetmek için yapılandırılmış bir yaklaşım sağlayan Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Siber Güvenlik Çerçevesi ile uyumlu olmasıdır (Dimakopoulou, 2024). Bu çerçeve, denizcilik kuruluşlarını siber olayları tanımlamaya, korumaya, tespit etmeye, bunlara yanıt vermeye ve bunlardan kurtulmaya teşvik etmektedir. Bu önlemleri uygulayarak işletmeler, olası siber tehditlere daha iyi hazırlanabilmekte ve güvenlik ve operasyonel verimlilik üzerindeki etkilerini azaltabilmektedir.

MSC.428(98) ayrıca, denizcilik personelini siber tehditleri etkili bir şekilde tanıma ve bunlara yanıt verme konusunda gerekli becerilerle donatmak için eğitim ve farkındalık programlarına olan ihtiyacı vurgulamaktadır. Bu ihtiyaçlar, gemi ve kıyı personeli arasında bir siber güvenlik farkındalığı kültürü oluşturmayı içermektedir. Denizcilik işletmeleri, personelin bilgi ve becerilerini geliştirerek siber olayların olasılığını önemli ölçüde azaltabilir ve genel siber güvenlik duruşlarını iyileştirebilir.

Dahası, MSC.428(98), gemi sahipleri, operatörler ve düzenleyici kurumlar dahil olmak üzere denizcilik sektöründeki paydaşlar arasında iş birliğini ve bilgi paylaşımını teşvik etmektedir. Bu iş birlikçi yaklaşım, en iyi uygulamaları geliştirmek ve siber olaylardan öğrenilen dersleri paylaşmak açısından oldukça önemlidir (McGillivary, 2018). Paylaşılan bilgi topluluğunu teşvik ederek, denizcilik sektörü, siber tehditlere karşı dayanıklılığını toplu olarak artırabilir ve dahil olan tüm paydaşlar için daha güvenli bir operasyonel ortam sağlayabilir.

2.3.3 Denizcilik sektöründe yaşanmış siber saldırı vakaları

Denizcilik sektöründe siber güvenlik, dijital teknolojilere olan bağımlılığın artması ve bunların getirdiği potansiyel güvenlik açıkları nedeniyle kritik bir endişe kaynağıdır. Denizcilik sektörünün dijitalleşmesi, siber güvenlik sorununu önemli ölçüde artırmıştır (Kayısoğlu vd., 2022). Denizcilik endüstrisindeki siber tehditlerden korunma, teknolojiyi, bilgiyi ve insan faktörünü kapsamakta olup, siber saldırıları anlamak ve azaltmak için kapsamlı bir yaklaşımı gerektirmektedir.

Sektörün siber saldırılara karşı savunmasızlığı, kimlik avı ve hedef odaklı kimlik avı da dahil olmak üzere dolandırıcılığı ana siber olay olarak tanımlayan ve siber güvenlik önlemlerine acil ihtiyaç olduğunu vurgulayan araştırma bulgularıyla vurgulanmıştır (Kuhn vd., 2021). Denizcilik BT departmanlarında teknik uzmanlık eksikliği ve farklı yerlerdeki birden fazla kuruluşun katılımı, denizcilik endüstrisinde siber güvenlik standartlarının oluşturulmasını daha da karmaşık hale getirmektedir.

Denizcilikteki dijital kontrol sistemleri siber saldırılara karşı giderek daha hassas hale gelmektedir ve buna bağlı olarak, denizcilik endüstrisini hedef alan siber olayların sayısı artmaktadır. Denizcilik endüstrisinde gelişen dijitalleşme, limanlara ve gemilere yönelik siber saldırılarda önemli bir artışa yol açarak, sektörde etkili siber risk yönetimine yönelik acil ihtiyacı vurgulamaktadır (Antonopoulos vd., 2022). Ayrıca, denizcilik sektörüne yönelik siber güvenlik araştırma ve azaltma yeteneklerinin eksikliği, deniz siber güvenliği risklerini ve tehditlerini ele almak için yeni araştırma yeteneklerinin geliştirilmesine yol açmıştır.

IMO, denizcilik navigasyonu ve radyo iletişim ekipmanı ve sistemleri için yeni standartlar geliştirmek amacıyla Uluslararası Elektroteknik Komisyonu (IEC) ile işbirliği yapmaktadır ve endüstrinin siber güvenliğin önemini kabul ettiğini önemle vurgulamaktadır (Sviličić vd, 2019). Denizcilik sektörünün verimliliği

artırmak ve modern zorluklarla başa çıkmak için teknolojiye artan bağımlılığı, siber ve siber fiziksel güvenliğin önemini artırmış ve sağlam siber güvenlik önlemlerinin oluşturulmasını zorunlu kılmıştır.

Siber güvenlik standartlarının eksikliği ve güvenli iletim protokollerinin bulunmaması, denizcilik siber güvenliğine yönelik önemli tehditler oluşturmakta, endüstride kapsamlı siber güvenlik politikalarına ve önlemlerine olan acil ihtiyacın altını çizmektedir (Wiseman, 2014).

Siber saldırı teknolojilerinin ve varyantlarının artmasıyla birlikte özellikle son yıllarda denizcilik sektörünü hedef alan tehdit sayısı ve sıkılığında da doğru orantılı bir artış söz konusudur. Bu saldırılar daha önceleri sadece doğrudan işletmeleri, bir başka deyişle kara departmanlarına ait ofisleri hedef almaktayken bugün limanlar ve dahası, seyir halindeki gemilere yönelik gerçekleşmektedir. Gemilere düzenlenen gelişmiş siber saldırılar, seyir cihazlarının uzaktan kontrol edilmelerine sebep olabileceği gibi, gemi adamlarının fiziksel yaralanmaları ve deniz kirliliği gibi daha vahim sonuçlar da doğurabilecek potansiyele sahiptir.

Siber saldırılar, siber korsanlar tarafından yapılabileceği gibi, yetkili devlet organları tarafından da gerçekleştirilebilmektedir. Bu sebeple saldırı türleri de gerek gelişmişlik gerekse de şiddet bakımından farklılık gösterebilmektedir. Siber saldırının etkisi, hedefe göre de değişiklik göstermektedir. Günümüzde siber saldırılar neticesinde yangınlar ve hatta patlamalara varacak tesirler oluşturmak mümkündür. Siber saldırıların sebepleri arasında en temel olanlar politik, ekonomik, dini, ego tatmini, intikam alma dürtüsü yer almaktadır (Keleştemur, 2015).

Günümüzde, özellikle otonom gemi projelerinin yaygınlaşmasıyla birlikte, son teknolojiyle donatılmış gemilerin, siber saldırılara karşı ne kadar zayıf olduğu da önemli bir tartışma konusu haline gelmektedir. Denizcilik sektörünü hedef almış, yaşanmış siber saldırı vakaları potansiyel saldırılara da ayna tutmaktadır.

IMO, denizcilik siber güvenliğini ele almanın aciliyetini kabul etmiş ve artan siber riskleri azaltmak için gelişmiş siber güvenlik önlemleri alınması çağrısında bulunmuştur. Son yıllarda siber saldırganlar denizcilik işletmelerini, gemileri ve kıyıdaki tesisleri hedef alan bir dizi siber olaylara maruz bırakmıştır (Kuhn vd., 2021).

Denizcilikteki siber tehditlerin benzersiz doğası, siber ve denizcilik faktörleri arasındaki karmaşık etkileşimi ele almak için özel risk değerlendirme çerçevelerinin geliştirilmesine yol açmıştır. Bu çerçeveler, denizcilik bağlamındaki siber olayların kapsamlı bir şekilde anlaşılmasını sağlamayı ve etkili siber risk yönetimini kolaylaştırmayı amaçlamaktadır.

Artan siber risklere yanıt olarak, yeni nesil denizcilik siber araştırma yeteneklerinin geliştirilmesine artan bir vurgu yapılmaktadır. Cyber-SHIP Laboratuvarı gibi girişimler, denizcilik sektöründeki siber tehditleri anlamak ve azaltmak için endüstriye, hükümete ve akademik camiaya gerekli araçları sağlamak üzere önerilmiştir (Tam vd., 2019).

2.3.3.1 Antwerp Limanı siber saldırısı

2009 yılında Belçika'nın Antwerp Limanı'nda gerçekleşen siber saldırı, liman operasyonlarını ciddi şekilde aksatmıştır. Siber korsanlar, limanın konteyner takip sistemine sızarak uyuşturucu kaçakçılığı için konteynerlerin yerlerini değiştirmiştir. Bu saldırı, limanın güvenliğini büyük ölçüde tehlikeye attı ve operasyonel süreçlerde ciddi bozulmalara yol açmıştır. Yetkililer, saldırının ardından güvenlik açıklarını tespit etmek ve benzer olayların önüne geçmek için kapsamlı bir soruşturma başlatmıştır.

Saldırganlar, konteynerleri izleyerek değerli yükleri belirleyip çalmayı başarmışlardır. Bu durum, liman güvenliği için büyük bir tehdit oluşturmuş ve limanın itibarını önemli ölçüde zedelemiştir. Bu siber vaka, liman yönetimlerinin sadece fiziksel güvenlik değil, aynı zamanda siber güvenlik konularında da hazırlıklı olmaları gerektiğini göstermiştir. Liman yetkilileri, saldırının ardından güvenlik önlemlerini artırarak operasyonel süreçlerin güvenliğini sağlamak için yeni protokoller geliştirmiştir (Seatrade Maritime, 2013).

2.3.3.2 Güney Kore sondaj platformuna kötü amaçlı yazılım saldırısı

2010 yılında, Güney Kore'deki bir inşaat sahasından Güney Amerika'ya giden bir sondaj platformu, kötü amaçlı yazılım saldırısına maruz kalmıştır. Bu saldırı, platformun kritik kontrol sistemlerine virüs bulaşmasına neden olmuştur. Saldırganlar, sondaj platformunun çeşitli bilgisayarlarına kötü amaçlı yazılım yükleyerek, operasyonel süreçleri ciddi şekilde aksatmıştır. Özellikle, Blowout

Preventer (BOP) sistemini kontrol eden bilgisayarlara bulaşan virüs, platformun güvenli ve verimli bir şekilde çalışmasını engellemiştir.

Saldırı sonucunda, sondaj platformunun operasyonlarını durdurmak ve sistemi temizlemek için 19 günlük bir kesinti yaşanmıştır. Bu tür kapatmaların günlük maliyeti yaklaşık 700.000 USD olarak tahmin edilmektedir; bu da toplamda 13.3 milyon USD'lik bir kayba yol açmıştır.

Olay, denizcilik sektöründe siber güvenliğin önemini ve kontrol sistemlerinin korunmasının ne kadar kritik olduğunu bir kez daha ortaya koymuştur. Şirket, olayın ardından siber güvenlik önlemlerini artırmak için önemli adımlar atmış ve çalışanlarına yönelik kapsamlı bir siber güvenlik eğitim programı başlatmıştır (Drilling Contractor, 2015).

2.3.3.3 Yunan denizcilik şirketine Wi-Fi üzerinden saldırı

2010-2011 yılları arasında bir Yunan denizcilik şirketi, merkez ofisindeki Wi-Fi ağı üzerinden gerçekleştirilen bir siber saldırıya maruz kalmıştır. Saldırganlar, şirketin IT sistemlerine sızarak gemilere ve seyir rotalarına ilişkin bilgileri ele geçmiştir. Bu bilgiler, Aden Körfezi'nde fiziksel korsan saldırıları planlamak ve yürütmek için kullanmıştır. Yerel korsanlar, gemilerin en savunmasız olduğu anları ve rotaları belirleyerek, saldırıları daha etkili hale getirebilmiştir.

Bu saldırılar sonucunda, şirket ciddi mali kayıplara uğramış ve güvenlik açıklarını gidermek için büyük çaba sarf etmek zorunda kalmıştır. Siber korsanlar, gemilere yönelik saldırılarını artırarak, denizcilik operasyonlarını aksatmış ve şirketin itibarına zarar vermiştir.

Olayın ardından, şirket siber güvenlik önlemlerini artırmak ve benzer olayların tekrarlanmasını önlemek için kapsamlı bir güvenlik stratejisi geliştirmiştir. Bu durum, denizcilik sektöründe siber güvenlik önlemlerinin ne kadar kritik olduğunu bir kez daha göstermiş ve diğer şirketlerin de güvenlik protokollerini gözden geçirmesine neden olmuştur (Safety4Sea, 2019).

2.3.3.4 İran Basra Körfezi'ndeki açık deniz platformuna siber saldırı

2012 yılında İranlı yetkililer, Basra Körfezi'ndeki bir açık deniz petrol platformunun iletişim ağlarına yönelik bir siber saldırı düzenlendiğini bildirmiştir. Bu saldırı, İran'ın petrol sektörü üzerindeki siber güvenlik tehditlerinin ciddiyetini

ortaya koymuştur. Saldırının ardından, İran'ın petrol bakanlığı ve Ulusal İran Petrol Şirketi'nin (NIOC) web siteleri ve diğer ilgili resmi siteler çevrimdışı hale gelmiştir. Bu kesinti, ülkenin petrol üretim ve ihracat faaliyetlerini geçici olarak aksatmıştır.

İran, saldırının ardından "siber kriz komitesi" kurarak bu tür tehditlerle başa çıkmak için acil önlemler almıştır. Yetkililer, saldırının bazı kullanıcı verilerini sildiğini kabul etmiş, ancak üretim ve ihracatın etkilenmediğini belirtmiştir. Bu olay, İran'ın Stuxnet saldırısının ardından siber güvenlik önlemlerini ne kadar ciddiye aldığını ve bu tür saldırılara karşı savunma kapasitelerini geliştirdiğini göstermiştir. İran'ın bu proaktif tepkisi, ülkedeki kritik altyapıları korumak için alınan güvenlik tedbirlerinin önemini bir kez daha vurgulamıştır (The Jerusalem Post, 2012).

2.3.3.5 Avustralya gümrük ve sınır koruma siber saldırısı

2012 yılında, Avustralya Gümrük ve Sınır Koruma'nın sistemlerine yönelik bir siber saldırı gerçekleşmiştir. Saldırganlar, gümrük işlemlerini izleyerek hangi konteynerlerin şüpheli olduğunu kontrol etme yeteneği kazanmıştır. Bu saldırı, sınır güvenliğini ciddi şekilde tehdit etmiş ve yetkililerin operasyonel verimliliğini önemli ölçüde düşürmüştür. Saldırganların verileri nasıl elde ettiği tam olarak belirlenemese de olayın ardından güvenlik protokolleri sıkılaştırılmıştır.

Bu olay, denizcilik sektöründe faaliyet gösteren devlet kurumlarının da siber saldırılara karşı ne kadar savunmasız olabileceğini konusunda önemli bir örnek teşkil etmektedir. Gümrük ve sınır koruma yetkilileri, saldırının ardından bilgi teknolojileri sistemlerini gözden geçirerek güvenlik açıklarını kapatmaya yönelik kapsamlı önlemler almıştır. Ayrıca, çalışanlarına yönelik siber güvenlik farkındalığı ve eğitim programları başlatarak benzer olayların tekrarlanmasını önlemeye çalışmıştır (Australian National Audit Office, 2014).

2.3.3.6 Windward raporu - AIS manipülasyonu ve kimlik sahtekarlığı

2014 yılında Windward tarafından yayımlanan bir rapor, 2012 ile 2014 yılları arasında tüm gemilerin yüzde birinin Otomatik Tanımlama Sistemi (AIS) iletimlerinde sahte kimlik bilgileri (IMO numaraları) sağladığını ortaya koymuştur. Ayrıca, gemilerin yüzde 25'inden fazlasının, zamanın en az yüzde 10'unda AIS'lerini devre dışı bıraktığı ("karartmaya başlama") tespit edilmiştir. Bu tür teknikler

genellikle kaçakçılık, terörizm, insan ticareti, yasadışı balıkçılık veya askeri çatışmalarla bağlantılı olarak kullanılmaktadır.

AIS sahtekarlığı ve manipülasyonu, denizcilik sektöründe büyük bir güvenlik tehdidi oluşturmaktadır. Windward'ın raporu, AIS verilerinin güvenilirliğinin giderek azaldığını ve manipülasyonların arttığını vurgulamaktadır. Gemiler, kimliklerini gizlemek veya faaliyetlerini saklamak için AIS verilerini kasıtlı olarak değiştirerek yetkililerin dikkatinden kaçmayı başarabilmektedir. Bu tür faaliyetler, deniz güvenliği ve uluslararası ticaret için ciddi riskler oluşturmaktadır (Windward, 2022).

2.3.3.7 Massachusetts Denizcilik Akademisi web sitesi hacklenmesi

2014 yılında Massachusetts Denizcilik Akademisi'nin web sitesi, İslami bir grup tarafından hacklenmiştir. Saldırganlar, web sitesinin içeriğini İslami mesajlarla değiştirmiştir (defacement). Bu olay, denizcilik eğitim kurumlarının da siber saldırılara karşı savunmasız olduğunu göstermiş ve eğitim kurumlarının güvenlik önlemlerini gözden geçirmesine yol açmıştır.

Yaşanan olayın ardından akademi yetkilileri, web sitesini tekrar güvenli hale getirmek ve benzer saldırılardan korunmak için kapsamlı önlemler almıştır. Akademi yetkilileri, saldırının ardından bilgi teknolojileri altyapılarını gözden geçirerek ve güvenlik önlemlerini artırarak benzer olayların tekrarlanmasını önlemeye çalışmıştır. Öğrencilere ve personele yönelik siber güvenlik eğitim programları başlatılmış ve farkındalık artırıcı faaliyetler düzenlenmiştir. Ayrıca, akademi web sitesinin güvenliğini sağlamak için yeni protokoller ve yazılım güncellemeleri uygulanmıştır (Boston Magazine, 2014).

2.3.3.8 ABD nükleer uçak gemisi içeriden saldırı

2014 yılında bir sistem yöneticisi, ABD'ye ait bir nükleer uçak gemisinde içeriden bir siber saldırı düzenlemiştir. Saldırgan, geminin IT sistemlerine sızarak kritik verilere erişim sağlamış ve operasyonel süreçlerini tehlikeye atmıştır. Bu olay, denizcilik sektöründe iç tehditlerin de ciddi bir sorun olduğunu ortaya koymuştur. Yetkililer, saldırının ardından güvenlik protokollerini gözden geçirmiş ve gerekli güncellemeleri uygulayarak, benzer olayların tekrarlanmasını önlemeye çalışmıştır.

Uçak gemisi yetkilileri, saldırının ardından bilgi teknolojileri üzerindeki prosedür ve politikalardan başka, teknik çalışmalar da uygulamıştır. Bunun dışında

insan faktörünün ne denli olduğu bilinci oluşmuş ve çalışanlarına yönelik siber güvenlik eğitim programları başlatarak farkındalık artırıcı faaliyetler düzenlemiştir (Data Breach Today, 2014).

2.3.3.9 Güney Kore'de 280 gemiye GPS karartması

2016 yılında Güney Kore'de yüzlerce uçak ve gemi, navigasyon sistemlerinde yaşanan sorunlar nedeniyle limana dönmek zorunda kalmıştır. Bu sorunların, Kuzey Kore tarafından gerçekleştirilen GPS karartma saldırılarından kaynaklandığı iddia edilmiştir. Kuzey Kore'nin, Güney Kore ve ABD'nin ortak askeri tatbikatları sırasında geniş çaplı GPS karartma sinyalleri gönderdiği tespit edilmiştir.

Bu saldırılar, gemilerin yanı sıra uçaklar ve kara taşıtları da dahil olmak üzere birçok ulaşım aracını etkilemiştir. Saldırılar, gemilerin güvenli seyir yapmasını engellemiş ve operasyonel süreçlerde ciddi aksamalara yol açmıştır. Güney Koreli yetkililer, bu saldırıların ardından GPS karartma sinyallerini tespit edip önlemek için çeşitli önlemler almıştır. Ancak, saldırıların arkasında doğrudan Kuzey Kore'nin olduğuna dair kesin deliller bulunamamış ve bu nedenle resmi bir suçlama yapılamamıştır.

Bu olay, denizcilik sektöründe GPS ve diğer navigasyon sistemlerinin güvenliğinin ne kadar kritik olduğunu bir kez daha ortaya koymuştur. Vaka, ayrıca siber saldırganların anonimliğini ne denli koruyabildiğini bir kez daha göstermiştir. Güney Kore, gelecekte benzer saldırılara karşı daha dirençli olmak için teknolojik altyapısını ve güvenlik protokollerini geliştirmeye yönelik adımlar atmış ve bunu bir devlet politikası haline getirmiştir (BBC, 2016).

2.3.3.10 Clarksons siber saldırısı

2017 yılında İngiliz gemi komisyoncusu Clarksons, ciddi bir siber saldırıya maruz kalmıştır. Saldırganlar, şirketin sistemlerine sızarak hassas bilgileri ele geçirmiş ve bu bilgilerin geri verilmesi için fidye talep etmiştir. Bu saldırı, Clarksons'ın bilgi güvenliği protokollerindeki bir zafiyetten yararlanarak gerçekleştirilmiştir. Siber saldırganların, kullanıcı hesaplarından birini ele geçirerek sisteme erişim sağladıkları tespit edilmiştir. Şirket, fidye taleplerine boyun eğmeyi reddetmiş ve saldırının hemen ardından soruşturma başlatmıştır.

Saldırı sonrasında Clarksons'ın hisselerinde yüzde 5'lik bir düşüş yaşanmıştır. Şirket, çalınan verilerin bir kısmını kurtarabilmek için siber güvenlik uzmanları ve hukuk otoriteleriyle işbirliği yapmıştır. Siber güvenlik uzmanlarınca yapılan sıkılaştırma çalışmaları sonrası şirket, bilgi güvenliği politikalarını da uygulayarak siber güvenlik duruşunu artırabilmiştir. Clarksons ayrıca, müşterilerine yönelik veri ihlali bildirimleri göndermiş ve gerekli hukuki adımları atmıştır (gCaptain, 2018).

2.3.3.11 MAERSK NotPetya saldırısı

2017 yılında gerçekleşen NotPetya siber saldırısı, Maersk Line dahil olmak üzere birçok büyük denizcilik şirketini etkilemiştir. Bu fidye saldırısı, operasyonel aksamaya ve büyük finansal kayıplara neden olmuştur. Maersk, bu saldırının etkilerini telafi etmek için önemli miktarda kaynak harcamış ve güvenlik protokollerini ciddi şekilde güncellemiştir. NotPetya saldırısı, denizcilik sektöründe siber güvenliğin ne kadar kritik olduğunu bir kez daha ortaya koymuş, önemli bir siber vakadır.

Saldırı, Maersk'in dünya genelindeki operasyonlarını geçici olarak durdurmasına neden olmuştur. Şirket, saldırının ardından sistemlerini yeniden yapılandırmak ve benzer olaylardan korunmak için kapsamlı bir strateji geliştirmiştir. Ayrıca, siber güvenlik uzmanlarıyla işbirliği yaparak güvenlik protokollerini gözden geçirmiş ve çalışanlarına yönelik eğitim programları düzenlemiştir. Maersk, bu saldırının ardından daha güçlü bir siber güvenlik altyapısı oluşturarak operasyonel faaliyetlerine kaldığı yerden devam etmiştir (Los Angeles Times, 2017)

2.3.3.12 COSCO Shipping Lines fidye yazılımı saldırısı

2018 yılında COSCO Shipping Lines'ın ABD ağı, bir fidye yazılımı saldırısına maruz kalmıştır. Bu saldırı, şirketin Kuzey Amerika operasyonlarını geçici olarak durdurmuş ve müşteri verilerinin tehlikeye girmesine neden olmuştur. COSCO, saldırının ardından sistemlerini yeniden yapılandırmak ve benzer saldırılardan korunmak için kapsamlı güvenlik önlemleri almıştır. Şirket ayrıca, bilgi teknolojileri altyapısını güçlendirmek ve siber güvenlik protokollerini güncellemek için önemli adımlar atmıştır.

COSCO, saldırının ardından operasyonel süreçlerini ve güvenlik önlemlerini gözden geçirmiştir. Şirket, çalışanlarına yönelik siber güvenlik eğitim programları

başlatarak benzer olayların tekrarlanmasını önlemeye çalışmıştır. Ayrıca, fidye yazılım saldırılarına karşı dirençli bir sistem oluşturmak için güvenlik yazılımlarını güncellemiş ve yeni protokoller geliştirmiştir. Bu olay, denizcilik sektöründe fidye yazılımı tehditlerinin bir kez daha ne kadar ciddi olabileceğini ve bu tür tehditlere karşı hazırlıklı olmanın önemini göstermiştir (Maritime Executive, 2018).

2.3.3.13 Barcelona Limanı siber saldırısı

Eylül 2018'de, Barcelona Limanına karşı ciddi bir siber saldırı düzenlenmiştir. Siber saldırganlar, limanın bilgisayar sistemlerini hedef alarak operasyonlarını aksatmış ve kargo işlemlerini ve idari fonksiyonları önemli ölçüde etkilemiştir. Liman yetkilileri, saldırıyı kontrol altına almak ve etkilerini hafifletmek için hemen harekete geçmiştir. Barcelona Liman Saldırısı, liman altyapısının güvenlik açıklarını ve sağlam siber güvenlik önlemlerinin önemini tekrar ortaya koymuştur.

Saldırının ardından, limanın BT ekibi normal operasyonları yeniden başlatmak ve etkilenen sistemleri güvence altına almak için yoğun bir şekilde çalışmak zorunda kalmıştır. İlgili siber vaka, büyük miktarda kargo ve veri işleyen büyük limanlarda kapsamlı siber güvenlik stratejilerinin gerekliliğini vurgulamaktadır. Barcelona Limanı, gelecekteki olayları önlemek için siber güvenlik altyapısına ve personel eğitimine yatırımını artırmak zorunda kalmıştır (Ports Europe, 2018).

2.3.3.14 San Diego Limanı siber saldırısı

2018 yılında San Diego Limanı, büyük bir fidye yazılımı saldırısına maruz kalmıştır. Saldırganlar, limanın IT sistemlerine sızarak kritik verilere erişim sağlamış ve operasyonel süreçlerin ciddi şekilde aksamasına sebep olmuştur. Bu saldırı, limanın operasyonlarını durma noktasına getirmiş ve ticari faaliyetleri büyük ölçüde etkilemiştir. Liman yetkilileri, saldırının ardından sistemlerini yeniden yapılandırmak ve benzer olaylardan korunmak için kapsamlı güvenlik önlemleri almıştır.

San Diego Limanı, saldırının ardından bilgi teknolojileri altyapısını güçlendirmek ve siber güvenlik protokollerini güncellemek için önemli adımlar atmıştır. Liman yetkilileri, çalışanlarına yönelik siber güvenlik eğitim programları başlatarak benzer saldırıların tekrarlanmasını önlemeye çalışmıştır. Bu eğitimler,

çalışanların siber tehditlere karşı daha bilinçli ve hazırlıklı olmalarını sağlamıştır. Ayrıca, fidye yazılımı saldırılarına karşı daha dirençli bir sistem oluşturmak için güvenlik yazılımlarını güncelledi ve yeni protokoller geliştirmiştir (Bank of Info Security, 2018).

2.3.3.15 New York Limanı'na girmesi engellenen gemi

2019 yılında büyük bir konteyner gemisi, bir fidye yazılımı saldırısına maruz kalmıştır. Bu saldırı geminin New York Limanı'na girmesini engellemiştir. Saldırganlar, geminin IT sistemlerine sızarak operasyonel süreçleri aksatmış ve liman yetkililerinin gemiyi güvenli bir şekilde limana yönlendirmesini engellemiştir. Bu olay, liman operasyonlarını ve ticaretini ciddi şekilde etkilemiş ve denizcilik sektöründe fidye yazılımı tehditlerinin ne denli tehlikeli olabileceğini bir kez daha göstermiştir.

Saldırının ardından, liman yetkilileri ve gemi operatörleri hızlı bir şekilde harekete geçerek güvenlik önlemlerini artırmıştır. Geminin IT sistemleri yeniden yapılandırılmış ve fidye yazılımı tehditlerine karşı daha dirençli hale getirilmiştir. Ayrıca, gemi mürettebatına yönelik siber güvenlik eğitim programları başlatılmış ve farkındalık artırıcı faaliyetler düzenlenmiştir. Bu olay, denizcilik sektöründe faaliyet gösteren diğer gemi operatörleri için de önemli dersler içermektedir (gCaptain, 2022).

2.3.3.16 Naantali Limanı tanker fidye yazılım saldırısı

2019 yılında Finlandiya'nın Naantali limanı yakınlarındaki bir petrol tankerinin yönetim sunucusuna fidye yazılımı bulaşmıştır. Bu saldırı sonucunda, yedekleme diski de silinmiş olup, bu vaka geminin operasyonel verilerini geri yüklemesini imkansız hale getirmiştir. Uzak Masaüstü Protokolü (RDP), bir USB cihazı veya bir e-posta eki gibi çeşitli saldırı vektörlerinin kullanıldığı düşünülmektedir.

Bu tür saldırılar, denizcilik sektöründe fidye yazılımlarının yarattığı ciddi tehditleri gözler önüne sermiş ve gemilerin operasyonel süreçlerinde ciddi aksamalara yol açmıştır. Aynı tanker, bu olaydan dört ay sonra tekrar aynı limanın yakınlarında enfekte olmuştur. Bu durum, saldırganların sistemlere tekrar erişim sağladığını ve gemi sistemlerini yeniden hedef aldığını göstermektedir.

Saldırıların ardından, gemi operatörleri güvenlik önlemlerini artırmak ve benzer olayların tekrarlanmasını önlemek için kapsamlı adımlar atmıştır. Bu tür olaylar, denizcilik sektöründe siber güvenliğin önemini bir kez daha vurguladı ve gemi operatörlerinin siber tehditlere karşı daha dikkatli ve hazırlıklı olmaları gerektiğini bir kez daha göstermektedir (Maritime Cybersecurity, 2023)

2.3.3.17 Hurtigruten siber saldırısı

Norveç'in ünlü yolcu gemisi firması Hurtigruten, 2020 yılında bir siber saldırıya uğramıştır. Saldırganlar, şirketin IT sistemlerine sızarak operasyonel süreçleri ciddi şekilde aksatmıştır. Bu saldırı, şirketin yolcu bilgileri ve operasyonel verilerini tehlikeye atmıştır. Hurtigruten, saldırının ardından sistemlerini yeniden yapılandırmak ve benzer olaylardan korunmak için kapsamlı güvenlik önlemleri almak zorunda kalmıştır.

Hurtigruten, saldırının ardından bilgi teknolojileri sistemlerini gözden geçirerek ve güvenlik protokollerini güncelleyerek benzer olayların tekrarlanmasını önlemeye çalışmıştır. Şirket, çalışanlarına yönelik siber güvenlik eğitim programları başlatmış ve farkındalık artırıcı faaliyetler düzenlemiştir. Ayrıca, IT sistemlerinin güvenliğini sağlamak için yeni protokoller ve yazılım güncellemeleri uygulamıştır (Offshore Energy, 2020).

2.3.3.18 CMA CGM fidye yazılımı saldırısı

2020 yılında Fransız konteyner taşımacılığı şirketi CMA CGM, büyük bir fidye yazılımı saldırısına maruz kalmıştır. Saldırganlar, şirketin Asya-Pasifik bölgesindeki daha küçük yan kuruluşlarının ağlarına sızarak kritik verilere erişim sağlamış ve operasyonel süreçleri aksatmıştır. Bu saldırı, şirketin küresel operasyonlarını ciddi şekilde etkilemiş ve CMA CGM'nin itibarını önemli ölçüde zedelemiştir.

CMA CGM, saldırının ardından sistemlerini yeniden yapılandırmak ve fidye yazılımı tehditlerine karşı daha dirençli hale getirmek için önemli adımlar atmak zorunda kalmıştır. Şirket, bilgi teknolojileri altyapısını güçlendirmek ve güvenlik protokollerini güncellemek için kapsamlı bir strateji geliştirmiştir. Ayrıca, çalışanlarına yönelik siber güvenlik eğitim programları başlatarak ve farkındalık

artırıcı faaliyetler düzenlemiş, böylelikle benzer olayların tekrarlanmasını önlemeye çalışmıştır (Theloadstar, 2020).

2.3.3.19 Mediterranean Shipping Company (MSC) siber saldırısı

2020 yılında, dünyanın en büyük denizcilik şirketlerinden biri olan Mediterranean Shipping Company (MSC), büyük bir siber saldırıya uğramıştır. Saldırganlar, şirketin IT sistemlerine sızarak kritik verilere erişim sağlamış ve operasyonel süreçleri aksatmıştır. Bu saldırı, MSC'nin küresel operasyonlarını ciddi şekilde etkilemiş olup, ticari faaliyetlerde büyük aksamalara neden olmuştur.

Şirket, saldırının ardından sistemlerini yeniden yapılandırmak ve benzer olaylardan korunmak için kapsamlı güvenlik önlemleri almıştır. MSC, saldırının ardından bilgi teknolojileri altyapısını güçlendirmek ve siber güvenlik protokollerini güncellemek için önemli adımlar atmıştır. Şirket, çalışanlarına yönelik siber güvenlik eğitim programları başlatarak benzer saldırıların tekrarlanmasını önlemeye çalışmıştır.

Bu eğitimler, çalışanların siber tehditlere karşı daha bilinçli ve hazırlıklı olmalarını sağlamıştır. Ayrıca, fidye yazılımı saldırılarına karşı daha dirençli bir sistem oluşturmak için güvenlik yazılımlarını güncelledi ve yeni protokoller geliştirmiştir (SeaTrade Maritime, 2020).

2.3.3.20 AIDA Cruises fidye yazılımı saldırısı

2020 yılında, Alman yolcu gemisi operatörü AIDA Cruises'ın Rostock'taki genel merkezi DoppelPaymer fidye yazılımı saldırısına maruz kalmıştır. Bu saldırı, şirketin bilgi teknolojileri sistemlerinde ciddi sorunlara yol açtı ve AIDA'yı birçok yolculuğunu iptal etmeye zorlamıştır. Saldırganlar, şirketin sistemlerine sızmayı başararak, verileri şifreledikten sonra fidye talep etmiştir.

AIDA Cruises, saldırının etkilerini hafifletmek ve sistemlerini geri yüklemek için siber güvenlik uzmanlarıyla iş birliği yapmak zorunda kalmıştır. Saldırının hemen ardından, şirketin operasyonları ciddi şekilde aksamış ve birçok müşteri mağdur olmuştur. Saldırının ardından, AIDA Cruises güvenlik önlemlerini artırmak ve benzer olayların tekrarlanmasını önlemek için kapsamlı adımlar atmıştır.

Şirket, çalışanlarına yönelik siber güvenlik eğitim programları başlatarak farkındalık artırıcı faaliyetler düzenlemiştir. Ayrıca, IT sistemlerinin güvenliğini

sağlamak için yeni protokoller ve yazılım güncellemeleri uygulanmıştır. Bu olay, denizcilik sektöründe fidye yazılımı tehditlerinin ne kadar ciddi olabileceğini ve bu tür tehditlere karşı hazırlıklı olmanın önemini bir kez daha göstermiştir (Cruise Law News, 2020).

2.3.3.21 Tynemouth Ryuk fidye yazılımı saldırısı

2020 yılında, İngiltere'nin Tynemouth kenti yakınlarında demirlemiş bir geminin gemi sunucusu ve birden fazla PC istemcisi, Ryuk fidye yazılımına maruz kalmıştır. Saldırganlar, geminin yönetim sunucusuna ve birçok PC'ye sızarak tüm verileri şifrelemiştir. Fidye yazılımı saldırısı sonucunda, gemideki tüm verilerin şifrelendiği ve kaybolduğu tespit edilmiştir.

Bu durum, gemi operasyonlarının ciddi şekilde aksamasına neden olmuş ve geminin normal faaliyetlerine devam edebilmesi için tüm sistemlerin yeniden yüklenmesi gerekmiştir. Olayın ardından, BT hizmet sağlayıcısından iki uzman gemiye gönderilmiştir.

Uzmanlar, sistemlerin tamamen yeniden yüklenmesi gerektiğini ve yedekleme disklerinin de silindiğini belirlemiştir. Ryuk fidye yazılımının yayılma yolları arasında Uzak Masaüstü Protokolü (RDP), bir USB cihazı veya bir e-posta eki olduğu düşünülmektedir (Cihat Aşan, 2023).

2.3.3.22 Houston Limanı siber saldırısı

2020 yılında, ABD'nin en büyük limanlarından biri olan Houston Limanı, gelişmiş bir siber saldırıya maruz kalmıştır. Saldırganlar, limanın BT sistemlerine sızarak kritik verilere erişim sağlamış ve operasyonel süreçleri ciddi şekilde aksatmıştır. Bu saldırı, limanın operasyonlarını durma noktasına getirmiş ve ticari faaliyetleri büyük ölçüde etkilemiştir. Liman yetkilileri, saldırının ardından sistemlerini yeniden yapılandırmak ve benzer olaylardan korunmak için kapsamlı güvenlik önlemleri almıştır.

Houston Limanı, saldırının ardından bilgi teknolojileri altyapısını güçlendirmek ve siber güvenlik protokollerini güncellemek için önemli adımlar atmıştır. Liman yetkilileri, çalışanlarına yönelik siber güvenlik eğitim programları başlatarak benzer saldırıların tekrarlanmasını önlemeye çalışmıştır.

Bu eğitimler, çalışanların siber tehditlere karşı daha bilinçli ve hazırlıklı olmalarını sağlamıştır. Ayrıca, fidye yazılımı saldırılarına karşı daha dirençli bir sistem oluşturmak için güvenlik yazılımlarını güncellenmiş ve yeni protokoller geliştirilmiştir (International Pipeline Resilience Organization, 2021).

2.3.3.23 Rotterdam Limanı siber saldırısı

2021 yılında, Avrupa'nın en büyük limanı olan Rotterdam Limanı, büyük bir siber saldırıya maruz kalmıştır. Saldırganlar, limanın IT sistemlerine sızarak kritik verilere erişim sağlamış ve operasyonel süreçleri ciddi şekilde aksatmıştır. Bu saldırı, limanın operasyonlarını durma noktasına getirmiş olup, ticari faaliyetleri büyük ölçüde etkilemiştir. Liman yetkilileri, saldırının ardından sistemlerini yeniden yapılandırmak ve benzer olaylardan korunmak için kapsamlı güvenlik önlemleri almıştır.

Liman yetkilileri, saldırının ardından BT altyapısını güçlendirmek ve siber güvenlik protokollerini güncellemek için önemli adımlar atmıştır. Liman yetkilileri, çalışanlarına yönelik siber güvenlik eğitim programları başlatarak benzer saldırıların tekrarlanmasını önlemeye çalışmıştır.

Bu eğitimler, çalışanların siber tehditlere karşı daha bilinçli ve hazırlıklı olmalarını sağlamıştır. Ayrıca, fidye yazılımı saldırılarına karşı daha dirençli bir sistem oluşturmak için güvenlik yazılımlarını güncelledi ve yeni protokoller geliştirilmiştir (Port Technology, 2022).

2.3.3.24 DSME veri ihlali

2021 yılında Güney Koreli gemi inşa şirketi Daewoo Shipbuilding & Marine Engineering (DSME), büyük bir veri ihlaline maruz kalmıştır. Saldırganlar, şirketin sistemlerine sızarak önemli miktarda veriyi ele geçirmiştir. Bu veriler arasında gemi tasarımları ve diğer hassas bilgiler yer almaktadır. DSME, bu saldırının ardından sistemlerini yeniden yapılandırmak ve benzer olaylardan korunmak için kapsamlı güvenlik önlemleri almıştır.

DSME, saldırının ardından bilgi teknolojileri altyapısını güçlendirmek ve siber güvenlik protokollerini güncellemek için önemli adımlar atmıştır. Şirket, çalışanlarına yönelik siber güvenlik eğitim programları başlatarak benzer saldırıların tekrarlanmasını önlemeye çalışmıştır.

Bu eğitimler, çalışanların siber tehditlere karşı daha bilinçli ve hazırlıklı olmalarını sağlamıştır. Ayrıca, güvenlik yazılımlarını güncelleyerek ve yeni protokoller geliştirerek fidye yazılımı saldırılarına karşı daha dirençli bir sistem oluşturulmuştur (Maritime Executive, 2021).

2.3.3.25 Carnival Corporation veri ihlali

2021 yılında Carnival Corporation, bir veri ihlali yaşamış ve bu olay, hem çalışanların hem de misafirlerin kişisel verilerinin çalınmasına neden olmuştur. Bu saldırı, şirketin operasyonlarını ve itibarını ciddi şekilde etkilemiştir. Carnival Corporation, saldırının ardından sistemlerini yeniden yapılandırmak ve benzer olaylardan korunmak için kapsamlı güvenlik önlemleri almıştır.

Saldırı, Carnival Corporation'ın dünya genelindeki operasyonlarını geçici olarak durdurmasına neden olmuştur. Şirket, saldırının ardından bilgi teknolojileri sistemlerini gözden geçirerek ve güvenlik protokollerini güncelleyerek benzer olayların tekrarlanmasının önüne geçmeye çalışmıştır.

Carnival Corporation yöneticileri ayrıca, çalışanlarına yönelik siber güvenlik eğitim programları başlatmış ve farkındalık eğitimleri düzenlemiş, böylelikle benzer olayların tekrarlanmasını önlemeye çalışmıştır (Cruise Mapper, 2021).

2.3.3.26 Nagoya Limanı LockBit fidye yazılımı saldırısı

2023 yılında Japonya'nın en büyük limanı olan Nagoya Limanı, LockBit fidye yazılımı saldırısına maruz kalmıştır. Saldırganlar, limanın IT sistemlerine sızarak operasyonel süreçleri ciddi şekilde aksatmıştır. Bu saldırı, liman operasyonlarının durmasına ve Toyota'nın ithalat-ihracat hatlarının askıya alınmasına neden olmuştur.

Nagoya Limanı yetkilileri, saldırının ardından sistemlerini yeniden yapılandırmak ve benzer olaylardan korunmak için kapsamlı güvenlik önlemleri almıştır. Liman yetkilileri, çalışanlarına yönelik siber güvenlik eğitim programları başlatarak benzer saldırıların tekrarlanmasını önlemeye çalışmıştır.

Bu eğitimler, çalışanların siber tehditlere karşı daha bilinçli ve hazırlıklı olmalarını sağlamıştır. Ayrıca, fidye yazılımı saldırılarına karşı daha dirençli bir sistem oluşturmak için güvenlik yazılımlarını güncellemiş ve yeni protokoller geliştirmiştir (Security Week, 2023).

2.3.4 IMO Denizcilik Siber Risk Yönetimi kılavuzu

IMO, Denizcilik Siber Risk Yönetimi kılavuzlarını yayınlayarak denizcilik endüstrisindeki siber güvenlik risklerini ele almada önemli bir rol oynamıştır. Özellikle, IMO, MSC-FAL.1/Circ.3/Rev.2 belgesi altında Denizcilik Siber Risk Yönetimi Kılavuzlarını yayınlamıştır. Bu kılavuzlar, denizcilik sektöründe siber risklerin yönetimi için yüksek düzeyde öneriler sunmakta olup, denizcilik operasyonlarını dijital tehditlere karşı korumak için siber güvenlik önlemlerinin önemini vurgulamaktadır (Bocayuva, 2021).

IMO'nun Denizcilik Siber Risk Yönetimi'ne yaptığı vurgu, denizcilik sektöründeki siber güvenlik zafiyetlerinin ele alınmasının kritik bir gereklilik olduğunu göstermektedir. IMO, siber risk yönetimi için en iyi uygulamaları belirleyen kılavuzlar sunarak, denizcilik sistemlerinin dayanıklılığını artırmayı ve güvenlik, emniyet ve operasyonel bütünlüğü tehlikeye atabilecek siber tehditlerden korumayı amaçlamaktadır.

IMO'nun denizcilik alanındaki siber güvenlik risklerini ele alma çabaları, kritik altyapı sektörlerinde siber güvenlik uygulamalarını güçlendirmeyi hedeflemektedir. MSC-FAL.1/Circ.3/Rev.2'de belirtilen kılavuzlar, denizcilik paydaşlarının siber riskleri etkili bir şekilde değerlendirmeleri, hafifletmeleri ve yönetmeleri için bir çerçeve sunmakta olup, denizcilik endüstrisinde siber güvenliğin artırılması genel hedefi ile uyumlu hale gelmektedir.

IMO, siber risk yönetimine odaklanmış, böylelikle siber güvenlikte en iyi uygulamaları teşvik ederek, denizcilik endüstrisinin genel güvenlik duruşunu güçlendirmeye ve denizcilik operasyonları üzerindeki siber tehditlerin etkisini azaltmaya katkıda bulunmaktadır (Goerlandt ve Montewka, 2015).

2.3.4.1 Köprüüstü seyir sistemleri

Küresel Navigasyon Uydu Sistemleri (GNSS) zafiyetleri, birçok denizcilik altyapısının kritik bileşenleri oldukları ve siber saldırılara karşı savunmasız oldukları için oldukça endişe vericidir (Farah vd., 2022). Çoğunlukla çeşitli teknolojileri ve sensörleri entegre eden köprü sistemlerinin birbirine bağlı doğası, gemilerin siber tehditlere maruz kalma riskini artırmaktadır. Bu da seyir sistemlerini tehlikeye atarak denizcilik operasyonlarını riske sokmaktadır (Kavallieratos ve Katsikas, 2020).

Köprü operasyonlarında siber-fiziksel sistemlere olan bağımlılık, siber saldırılarla ilişkili riskleri hafifletmek için güçlü siber güvenlik önlemleri gerektiren karmaşıklıklar ve zafiyetler ortaya çıkarmaktadır. Denizcilik operasyonlarının artan dijitalleşmesi, köprü sistemlerinin karşı karşıya kaldığı siber riskleri artırmış olup, siber güvenliğe yönelik proaktif bir yaklaşımı zorunlu kılmaktadır.

Entegre Köprü Sistemleri (IBS) bileşenlerine yönelik siber güvenlik değerlendirmeleri sayesinde, karıştırma, aldatma ve ele geçirme gibi çeşitli siber saldırı teknikleri ile istismar edilebilecek zafiyetleri tespit edilmiştir (Mednikarov vd., 2020). Denizcilik endüstrisince, verimliliği ve sürdürülebilirliği artırmak için teknolojik gelişmeleri benimsenmeye devam ettikçe, köprü sistemlerindeki siber risklerin ele alınması, denizcilik operasyonlarının güvenliğini ve emniyetini sağlamak için giderek daha kritik hale gelmektedir.

2.3.4.2 Yük taşıma ve yönetim sistemleri

Yük taşıma sistemlerindeki zafiyetler, siber saldırılar yoluyla istismar edilebilir ve bu durum, yük dağıtımı ve lojistik süreçlerinde kesintilere yol açabilir. Tedarik zinciri BT altyapısının dinamik doğası, sürekli donanım ve yazılım değişiklikleri ile birleştiğinde, denizcilik sektöründeki yük taşıma sistemlerinin karşı karşıya olduğu gelişen siber tehditleri ele almak için risk yönetimi stratejilerinin yeniden değerlendirilmesini gerektirir.

Yük taşıma sistemleri, lojistik zincirler içinde karmaşık taşıma merkezlerine dönüştükçe, siber güvenlik önlemlerinin entegrasyonu, yük operasyonlarını siber risklere karşı korumak ve mal akışının kesintisiz devam etmesini sağlamak için zorunlu hale gelmektedir (John ve diğerleri, 2014).

Yük taşıma ve yönetim sistemlerinin kritik denizcilik altyapısı ile olan bağlantısı, yük operasyonlarının bütünlüğünü ve güvenliğini tehlikeye atabilecek siber tehditlere maruz bırakmaktadır. Küresel Navigasyon Uydu Sistemi (GNSS), Elektronik Harita Gösterim ve Bilgi Sistemi (ECDIS) ve kıyı kontrol merkezlerindeki (SCC) iletişim cihazları gibi alt sistemler, yük taşıma sistemleri içinde özellikle savunmasız bileşenler olarak tanımlanmıştır (Tusher vd., 2022).

Bu savunmasız bölümleri hedef alan siber saldırılar, yük yönetimi süreçlerini kesintiye uğratabilir, seyir sistemlerini tehlikeye atabilir ve iletişim kanallarını

tehlikeye atabilir. Bu da yük operasyonlarını siber tehditlerden korumak için sağlam siber güvenlik önlemlerinin uygulanmasının önemini vurgulamaktadır.

2.3.4.3 Pervane ve makine yönetimi ile güç kontrol sistemleri

Pervane ve makine yönetiminde siber-fiziksel sistemlerin entegrasyonu, kritik sistemlerin güvenilirliğini ve işlevselliğini tehlikeye atan karmaşıklıklar ve bağımlılıklar oluşturur ve gemilerin siber tehditlere maruz kalma riskini artırmaktadır. Pervane sistemleri ileri teknolojileri bünyesine kattıkça, siber risklere karşı koruma sağlamak ve denizcilik ortamlarında tahrik ve makine yönetim sistemlerinin sorunsuz çalışmasını temin etmek için sağlam siber güvenlik önlemlerine olan ihtiyaç daha da önemli hale gelmektedir.

Güç kontrol sistemlerinin kritik denizcilik altyapısı ile olan bağlantısı, onları tahrik ve makine operasyonlarının bütünlüğünü ve güvenilirliğini tehlikeye atabilecek siber tehditlere maruz bırakmaktadır. Güç kontrol sistemlerini hedef alan siber saldırılar, tahrik mekanizmalarını, makine yönetim süreçlerini ve güç dağıtım sistemlerini kesintiye uğratarak gemi operasyonlarına önemli riskler oluşturabilir (Polatidis vd., 2018).

Güç kontrol sistemlerindeki, GNSS ve iletişim cihazları gibi, zafiyetler onları siber tehditlere karşı savunmasız hale getirir ve gemilerin pervane ve makine işlevlerini etkileyebilir. Bu durum, denizcilik ortamlarında güç kontrol sistemlerini korumak için sağlam siber güvenlik önlemlerinin uygulanmasının önemini vurgulamaktadır.

2.3.4.4 Erişim kontrol sistemleri

Erişim kontrol sistemleri, siber saldırılar yoluyla istismar edilebilir ve bu durum, kritik denizcilik altyapısına ve hassas verilere yetkisiz erişime yol açabilir. Erişim kontrol sistemlerinin temel denizcilik varlıkları ile olan bağlantısı, gemilerin siber tehditlere maruz kalma riskini artırır ve erişim kontrol mekanizmalarının gizliliğini, bütünlüğünü ve kullanılabilirliğini tehlikeye atar (Cherdantseva vd., 2016).

Erişim kontrol sistemleri daha sofistike ve birbirine bağlı hale geldikçe, siber risklere karşı koruma sağlamak ve denizcilik varlıklarının güvenli erişim yönetimini

temin etmek için sağlam siber güvenlik önlemlerine olan ihtiyaç daha da önemli hale gelmektedir.

Erişim kontrol sistemlerinde siber-fiziksel sistemlerin entegrasyonu, gelişen siber tehditlere yönelik proaktif risk yönetimi stratejileri gerektiren karmaşıklıklar ve zafiyetler oluşturmaktadır. Erişim kontrol sistemleri, sosyal mühendislik ve yetkisiz erişim girişimleri ile istismar edilebilir.

2.3.4.5 Yolcu hizmetleri ve yönetim sistemleri

Yolcu hizmetleri için erişim kontrol sistemlerine yönelik siber saldırılar, yolcu verilerine yetkisiz erişime yol açabilir, yolcu güvenliğini tehlikeye atabilir ve hizmet yönetim süreçlerinde kesintilere neden olabilir. Kritik denizcilik altyapısı ile bağlantılı yolcu hizmet sistemleri, gemilerin siber tehditlere maruz kalma riskini artırır, yolcu bilgileri ve hizmet operasyonlarının gizliliğini ve bütünlüğünü tehlikeye atar (Ali vd., 2021).

Yolcu hizmetleri ve yönetim sistemleri daha gelişmiş ve birbirine bağlı hale geldikçe, siber risklere karşı koruma sağlamak ve denizcilik ortamlarında yolcu hizmetlerinin güvenli ve verimli yönetimini sağlamak için sağlam siber güvenlik önlemlerine ilişkin gerekler de daha fazla önem arz etmektedir.

Yolcu hizmetleri ve yönetim sistemlerindeki siber-fiziksel sistemlerin entegrasyonu, gelişen siber tehditlere yönelik proaktif risk yönetimi stratejileri gerektiren karmaşıklıklar ve zafiyetler ortaya çıkarmaktadır. Erişim kontrol bileşenleri, sahte saldırılar ve yetkisiz erişim girişimleri gibi çeşitli siber saldırı teknikleriyle istismar edilebilir, bu da yolcu güvenliği ve hizmet yönetiminde riskler oluşturmaktadır (Androjna ve Perkovič, 2021).

2.3.4.6 Yolcuya yönelik genel ağlar

Kritik denizcilik altyapısı ile bağlantılı yolcuya yönelik genel ağlar, gemilerin siber tehditlere karşı savunmasızlığını artırır, bu da hizmet yönetim süreçlerinde kesintilere ve yolcu güvenliğinin tehlikeye atılmasına yol açabilir (Yu vd., 2023). Yolcuya yönelik genel ağlar daha entegre ve teknolojik olarak gelişmiş hale geldikçe, siber risklere karşı koruma sağlamak ve denizcilik ortamlarında yolcu hizmetlerinin güvenli ve verimli yönetimini sağlamak için sağlam siber güvenlik önlemlerinin alınması gerekliliği de doğmaktadır.

Yolcu hizmetleri ve yönetim sistemlerindeki siber-fiziksel sistemlerin entegrasyonu, gelişen siber tehditlere yönelik proaktif risk yönetimi stratejileri gerektiren karmaşıklıklar ve zafiyetler ortaya çıkarmaktadır. Genel ağlara yönelik yaygın siber saldırılar, kod enjeksiyonu, kurcalama ve değiştirme, ortadaki adam ve kötü ikiz saldırıları gibi, yolcu güvenliği ve hizmet yönetiminde riskler oluşturmaktadır (Annarelli ve Palombi, 2021).

2.3.4.7 İdari ve mürettebat refah sistemleri

Bu sistemler, mürettebat yönetimi, maaş bordrosu, programlama ve gemideki personel için refah hizmetleri gibi işlevleri kapsar. IMO, siber riskler ve tehditler hakkında farkındalık yaratmanın aciliyetini kabul etmiş ve siber risklerin onaylı güvenlik yönetim sistemlerinde dikkate alınmasının önemini vurgulamıştır. Böylece denizcilik operasyonlarının siber tehditlere karşı dayanıklılığı artırılabilir (Larsen ve Lund, 2021). Siber tehditler, denizcilik endüstrisinde idari ve mürettebat refah sistemlerine yönelik önemli bir risk oluşturmakta, operasyonel verimliliği ve mürettebat üyeleri ile idari personelin refahını etkilemektedir.

İdari ve mürettebat refah sistemlerindeki siber-fiziksel sistemlerin entegrasyonu, gelişen siber tehditlere yönelik proaktif risk yönetimi stratejileri gerektiren karmaşıklıklar ve zafiyetler ortaya çıkarır. İdari ve mürettebat refah sistemlerinde siber riskleri proaktif olarak ele alarak ve sağlam siber güvenlik önlemlerini entegre ederek, denizcilik endüstrisi mürettebat refah hizmetlerinin güvenlik duruşunu güçlendirebilir, kritik altyapıyı koruyabilir ve denizcilik ortamlarında idari operasyonların verimli yönetimini sağlayabilir (Kayisoglu vd., 2022).

2.3.4.8 İletişim sistemleri

Denizcilik endüstrisinin iletişim sistemlerine olan bağımlılığı önemli ölçüde artmış olup, siber riskler konusunda artan bir endişe yaratmıştır. Hackerlar, siber zafiyetleri nedeniyle denizcilik sektörünü giderek daha fazla hedef almaktadır. Bu zafiyetler, siber ve denizcilik faktörlerinin benzersiz bir karışımını dikkate alan özel bir risk değerlendirme çerçevesine duyulan ihtiyacı vurgulamaktadır (Tam ve Jones, 2019).

IMO tarafından belirlenen yönergeler, denizcilik operasyonlarını, güvenliği ve emniyeti tehlikeye atabilecek dijital tehditleri azaltmak için Denizcilik Siber Risk Yönetimi'nin önemini vurgulamaktadır (Çetin ve Köseoğlu, 2020). Ayrıca, denizcilik endüstrisindeki dijitalleşmenin gelişmesi, limanları ve gemileri hedef alan siber saldırılarda bir artışa yol açmış olup, siber risk yönetimine yönelik proaktif bir yaklaşımı zorunlu kılmaktadır (Antonopoulos vd., 2022).

Denizcilik endüstrisinin dijitalleşmesi, GNSS gibi hayati altyapıları siber tehditlerden korumak için sağlam siber güvenlik önlemlerine duyulan ihtiyacı vurgulamakta ve sektörün siber saldırılara karşı savunmasızlığını göstermektedir (Farah vd., 2022).

3. YÖNTEM

Bu bölümde, araştırmanın amacı ve önemi tartışılmakta, aynı zamanda araştırma yönteminin oluşturulmasında kullanılan modeller ve yöntemler detaylı bir şekilde ele alınmaktadır. Bu kapsamda, araştırmanın temel hedefleri doğrultusunda izlenecek bilimsel yaklaşım belirlenmekte ve bu yaklaşımın teorik temelleri ile uygulamada kullanılacak metodolojik araçlar incelenmektedir.

3.1 Nitel ve Nicel Araştırma Yöntemi

Nitel araştırma, incelenen konuya yaklaşarak yeni ve anlamlı ayrımlar yaparak bir olgunun daha derin anlaşılmasını amaçlayan yinelemeli bir süreci içerir (Aspers ve Corte, 2021). Nicel araştırmaya kıyasla daha az yapılandırılmış, daha açık uçlu ve esnek olmasıyla karakterize edilir. Nitel araştırma yöntemleri, araştırmacıların yaklaşımlarını verilere ve örneğe uyacak şekilde uyarlamalarına olanak tanır ve derinlemesine araştırma için güçlü bir araç sağlar (Köhler vd., 2018).

Nicel araştırma ise bir veri seti içindeki ilişkileri, kalıpları ve eğilimleri ölçmek için sayısal verilerin toplanmasını ve analizini içerir. Tekrarlanabilirliği ve istatistiksel geçerliliği sağlamak için genellikle yapılandırılmış ve katı bir metodoloji izler (Teti ve Abbott, 2023). Nicel araştırmalar, verileri toplamak ve analiz etmek için sıklıkla vaka çalışmalarını ve küçük N tasarımlarını kullanır. Nicel araştırma, veri toplamak için ölçüm yoluyla test edilen bir hipotez veya kavramla başlar. Bu veriler ise çıkarımlarda bulunmak ve bir sonuca varmak için kullanılır (Greenhalgh ve Taylor, 1997).

Çizelge 3.1: Araştırma Yaklaşımları Arasındaki Farklılıklar

Öge	**Nitel**	**Nicel**
Sosyal teori	Eylem	Yapı
Yöntemler	Gözlem, görüşme	Deney, anket
Soru	X nedir? (sınıflandırma)	X kaç tane? (sayısal belirleme)
Akıl yürütme	Tümevarım	Tümdengelim
Örnekleme yöntemi	Teorik	İstatistiksel
Güçlü yan	Geçerlilik	Güvenilirlik

3.2 Hibrit Araştırma Yöntemi

Karma yöntem araştırması olarak da bilinen hibrit araştırma, bir araştırma probleminin daha kapsamlı anlaşılmasını sağlamak için nitel ve nicel araştırma yaklaşımlarının tek bir çalışma içerisinde bütünleştirilmesini içerir (Campbell vd., 2012). Bu yöntem, çeşitli veri toplama yöntemleri, analiz teknikleri ve çıkarım stratejileri kullanarak hem nitel hem de nicel araştırmanın güçlü yönlerini birleştirir. Nitel ve nicel verileri entegre ederek, araştırmacılar karmaşık olaylara ilişkin daha derin bir anlayış kazanabilir, bulgularının geçerliliğini artırabilir ve sonuçları desteklemek için hesaba dayalı tahmin üretimine yardımcı olur.

Hibrit araştırma modeli, araştırmacıların niteliksel ve niceliksel yöntemlerin ilgili güçlü yönlerinden yararlanmasına olanak tanıyarak araştırma sorularının daha bütünsel bir şekilde araştırılmasına olanak tanır. Çeşitli veri kaynaklarının ve analiz tekniklerinin entegrasyonu, çalışma bulgularının kesinliğini ve geçerliliğini artırır (Guetterman vd., 2015).

Çoklu bakış açıları ve içgörüler sağlayarak karmaşık olayların incelikli bir şekilde anlaşılmasını kolaylaştırır. Nitel ve nicel yaklaşımların birleşimi, ayrı ayrı kullanıldığında her yöntemin doğasında bulunan sınırlamaların azaltılmasına yardımcı olur. Metodolojinin, araştırma problemine uyacak şekilde uyarlama esnekliği sunar, böylece çalışmanın derinliğini ve genişliğini artırır (Sells vd., 1995).

3.3 MITRE ATT&CK Çerçevesi

MITRE ATT&CK çerçevesi, siber güvenlik profesyonelleri için kritik bir kaynaktır ve düşmanca taktikleri, teknikleri ve prosedürleri (TTP'ler) anlamak için yapılandırılmış bir yaklaşım sağlar. Çerçeve içinde özetlenen saldırı yeteneklerine sıklıkla çok dikkat edilse de MITRE ATT&CK üzerinden türetilen savunma stratejileri de aynı derecede önemlidir.

Bu stratejiler, kuruluşların olası saldırı vektörlerini ilgili savunma önlemlerine etkili bir şekilde eşleyerek siber güvenlik duruşlarını güçlendirmelerini sağlamaktadır. MITRE ATT&CK çerçevesinin temel avantajlarından biri, saldırı tekniklerinin test edilmiş savunma yöntemleriyle eşleştirilmesini kolaylaştırma yeteneğidir. Bu ikilik, kuruluşların gerçek dünya saldırı senaryolarından bilgi alan kapsamlı savunma stratejileri geliştirmelerine olanak tanır.

Çerçeve çeşitli saldırı tekniklerini, bir saldırı yaşam döngüsünün aşamalarını yansıtan matrislere kategorize ederek, savunucuların yanıtlarını farklı saldırı senaryolarının olasılığına ve etkisine göre önceliklendirmesini sağlamaktadır (Georgiadou vd., 2021). Çerçeve ayrıca, etkili bir savunma stratejisinin ayrılmaz bileşenleri olarak sürekli izleme ve tehdit avcılığının önemini vurgulamaktadır.

Bir ağ içinde tehlikeye ilişkin göstergeleri aktif olarak arayarak, kuruluşlar potansiyel tehditleri önemli olaylara dönüşmeden önce belirleyebilir. Bu proaktif yaklaşım, saldırganların yeni güvenlik açıklarını istismar etmek için yöntemlerini sürekli olarak uyarladığı günümüzün hızla gelişen tehdit ortamında önemlidir.

Yapılan son araştırma sonuçlarında da görüldüğü üzre, dijital adli bilişim tekniklerinin dahil edilmesi, dijital eserleri analiz ederek ve kural tabanlı akıl yürütmeyi uygulayarak devam eden siber saldırıların erken tespitine daha da yardımcı olmaktadır (Dimitriadis vd., 2023).

3.4. MITRE CAPEC Çerçevesi

MITRE CAPEC çerçevesi, çeşitli alanlarda siber tehditleri anlamak ve hafifletmek için önemlidir. Araştırmacılar, CAPEC'i zafiyetleri saldırı kalıplarına bağlamak için kullanarak potansiyel tehditlerin ve ilgili hafifletme stratejilerinin kapsamlı bir analizini yapmışlardır. CAPEC, güvenlik ihlallerinin sistematik bir şekilde anlaşılmasına ve etkili savunma mekanizmalarının geliştirilmesine yardımcı olan yapılandırılmış bir yaklaşım sunmaktadır (Li vd., 2016).

CAPEC'in, MITRE ATT&CK Matrix ve NIST Cybersecurity Framework gibi diğer siber güvenlik çerçeveleriyle entegrasyonu, genel siber tehdit istihbaratı ve risk değerlendirme yeteneklerini artırır (Kwon vd., 2020). CAPEC saldırı kalıplarının CVE zafiyet bilgisiyle izlenmesi, doğal dil işleme teknikleri kullanılarak, farklı siber güvenlik depolarının birbirine bağlılığını ve CAPEC'in kapsamlı tehdit analizi için değerini göstermiştir (Kanakogi vd., 2021).

CAPEC'in güvenlik gereksinimleri analizine katkısı, bilinen saldırı kalıplarına dayalı olarak güvenlik önlemlerinin belirlenmesi ve önceliklendirilmesi konusunda çok yönlülüğünü vurgulamaktadır. Genel olarak, CAPEC, siber risklerin proaktif yönetimine ve sağlam siber güvenlik stratejilerinin geliştirilmesine önemli ölçüde katkıda bulunan temel bir kaynak olarak ortaya çıkmaktadır.

Denizcilik endüstrisi, etkili risk yönetimi için sağlam çerçeveler ve yöntemlerin uygulanmasını gerektiren çeşitli siber risklerle karşı karşıyadır. Bu tür bir çerçeveye en iyi örneklerden biri, siber saldırı taktikleri ve teknikleri hakkında kapsamlı bir bilgi tabanı sunan MITRE ATT&CK Framework'tür (Xiong vd., 2021). Denizcilik işletmeleri, MITRE ATT&CK Matrix'i kullanarak, topluluk bazında kullanılabilecek bir siber tehdit istihbarat ağı oluşturabilir ve gelişen siber tehditlere karşı proaktif savunma stratejileri geliştirebilir.

Ek olarak, Cyber Kill Chain modeli, siber tehditleri anlama ve analiz etme konusunda yapılandırılmış bir yaklaşım sunarak, denizcilik varlıklarının potansiyel saldırı vektörlerini belirlemelerini ve riskleri etkin bir şekilde azaltmak için önleyici güvenlik önlemleri sağlar (Kim vd., 2018). MITRE ATT&CK Framework ve Cyber Kill Chain modeli ile birlikte, STRIDE modeli, denizcilik endüstrisindeki iletişim sistemlerindeki güvenlik tehditlerini belirlemek ve kategorize etmek için sistematik bir yöntem sunmaktadır.

Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service ve Elevation of Privilege'e dayalı tehditleri değerlendirerek, zafiyetleri proaktif olarak ele almak ve iletişim sistemlerinin dayanıklılığını artırmak mümkündür. Ayrıca, Diamond Model, düşman faaliyetlerini, altyapıyı, yetenekleri ve hedefleri haritalayarak siber tehditleri analiz etmek için yapılandırılmış bir yaklaşım sunmakta ve denizcilik varlık sahiplerine siber ve fiziksel güvenlik zafiyetlerini etkin bir şekilde değerlendirmeleri ve hafifletmeleri için değerli içgörüler sağlamaktadır (Progoulakis vd., 2021).

DREAD ve OWASP çerçeveleri, denizcilik endüstrisinde siber güvenlik uygulamalarını geliştirmeye yönelik değerli katkılar sunmaktadır. DREAD, hasar, tekrarlanabilirlik, istismar edilebilirlik, etkilenen kullanıcılar ve keşfedilebilirlik üzerine odaklanarak, risk değerlendirmesi için yapılandırılmış bir yaklaşım ve denizcilik işletmelerinin potansiyel tehditlerin ciddiyetine dayalı olarak güvenlik önlemlerini etkili bir şekilde önceliklendirmesini sağlar.

Denizcilik işletmeleri DREAD modelini kullanarak, varlıklarına yönelik kritik zafiyetlerini ele almak için kaynaklarını verimli bir şekilde tahsis edebilir ve böylece genel siber güvenlik duruşlarını güçlendirebilir. Öte yandan, OWASP, güvenli yazılım geliştirme için temel yönergeler ve en iyi uygulamalar sunarak,

denizcilik uygulamaları ve sistemlerinin yaygın web tabanlı saldırılara karşı dayanıklı olmasını sağlamaktadır (Tam ve Jones, 2019). OWASP önerilerine uyarak, denizcilik sektörü dijital altyapısının güvenliğini artırabilir ve siber tehdit riskini etkili bir şekilde azaltabilir.

DREAD ve OWASP çerçevelerini denizcilik siber güvenlik stratejilerine entegre etmek, endüstrinin siber tehditlere karşı dayanıklılığını önemli ölçüde artırabilir. DREAD'in risk değerlendirme yeteneklerinden ve OWASP'nin güvenli geliştirme uygulamalarından yararlanarak, denizcilik işletmelerini iletişim sistemlerindeki, kritik altyapılardaki ve yazılım uygulamalarındaki zafiyetleri proaktif olarak tanımlayabilir, değerlendirebilir ve hafifletebilir (Farah vd., 2022).

Bu entegre yaklaşım, denizcilik sektörünün siber olaylara karşı sağlam bir siber güvenlik çerçevesi oluşturmasına ve denizcilik operasyonlarının sürekliliğini sağlamasına olanak tanır. DREAD ve OWASP'nin güçlerini birleştirerek, denizcilik endüstrisi savunmalarını güçlendirebilir ve siber riskleri etkili bir şekilde azaltarak denizcilik operasyonlarının güvenliğini ve bütünlüğünü artan dijital ortamda sağlayabilir.

ISO 27001 ve ISO 31000, denizcilik endüstrisinde bilgi güvenliği ve etkili risk yönetimini sağlamak için uygulanabilecek kritik standartlardır. ISO 27001, bilgi güvenliği yönetim sistemlerine odaklanarak, işletmelerin bilgi güvenliği süreçlerini kurmalarını, uygulamalarını, sürdürmelerini ve sürekli olarak iyileştirmelerini sağlamak için yapılandırılmış bir yaklaşım sunar (Pecina vd., 2011). ISO 27001 yönergelerine uymak, denizcilik şirketlerinin siber güvenlik duruşlarını geliştirmelerine, hassas verileri korumalarına ve siber tehditlerle ilişkili riskleri azaltmalarına olanak tanır.

Öte yandan, ISO 31000, denizcilik işletmelerinin çeşitli operasyonel yönlerdeki riskleri etkili bir şekilde tanımlamalarını, değerlendirmelerini ve ele almalarını sağlayan kapsamlı bir risk yönetimi çerçevesi sunar (Papageorgiou vd., 2023). ISO 31000'i risk yönetimi uygulamalarına entegre etmek, denizcilik varlıklarının potansiyel tehditleri proaktif olarak ele almasını, karar verme süreçlerini iyileştirmesini ve genel operasyonel dayanıklılığı artırmasını sağlar.

ISO 27001 ve ISO 31000'in denizcilik endüstrisindeki önemi, kritik varlıkların ve operasyonların güvence altına alınması için standartlaştırılmış

yaklaşımlar sağlamalarında yatmaktadır. ISO 27001 sertifikasyonu, bilgi güvenliği best praactice'lerine bağlılığı göstererek, denizcilik sektöründe paydaşlar, müşteriler ve düzenleyici kuruluşlar arasında güven oluşturmaktadır (Shohoud, 2023).

ISO 27001'i uygulamak, denizcilik işletmelerinin sağlam bir bilgi güvenliği yönetim sistemi kurmalarına, siber tehditleri azaltmalarına ve endüstri düzenlemelerine uyumu sağlamalarına yardımcı olmaktadır. Benzer şekilde, ISO 31000, denizcilik işletmelerinin riskleri etkili bir şekilde tanımlamalarını ve yönetmelerini sağlar, bu da onların bilinçli kararlar almalarını, kaynakları önceliklendirmelerini ve belirsizlikler ve tehditlerle karşı karşıya kaldıklarında operasyonel dayanıklılıklarını artırmalarına yardımcı olur.

ISO 31000'in benimsenmesi, denizcilik işletmeleri içinde risk bilincine sahip bir kültürü teşvik ederek proaktif risk yönetimi uygulamalarını destekler ve dinamik ve zorlu bir denizcilik ortamında sürdürülebilir iş operasyonlarını sağlar. MITRE CAPEC kendi başına bir çerçeve olmasa da denizcilik sektörü için özel olarak geliştirilmiş bir metodolojinin altyapısını oluşturmak için kullanılabilir.

3.5 MITRE CAPEC Saldırı Vektörleri

Siber güvenlik ve denizcilik alanlarının karmaşık ve özel doğası nedeniyle, siber risklerin doğru bir şekilde değerlendirilmesi, sistematik bir yaklaşım kullanılmadan son derece zorlu olabilir. Araştırmamız, siber risk değerlendirmelerinde öznellikten kaynaklanan yanlılıkları azaltarak, uzman yargısına olan bağımlılığı hafifletmeyi amaçlamaktadır. Bu tez çalışmasında MITRE ATT&CK çerçevesindeki saldırı yöntemleri incelenmiş ve denizcilik sektöründe etkili olabilecek MITRE CAPEC saldırı yüzeyleri tanımlanmıştır. Denizcilik sistemlerine uyarlanmış metodolojimiz, CAPEC 1000 - Saldırı Mekanizmaları temelinde kategorize edilmiştir:

1. Aldatıcı Etkileşimler - (156)
2. Mevcut İşlevselliği Kötüye Kullanma - (210)
3. Veri Yapılarını Manipüle Etme - (255)
4. Sistem Kaynaklarını Manipüle Etme - (262)
5. Beklenmedik Öğeler Enjekte Etme - (152)
6. Olasılıksal Teknikleri Kullanma - (223)

7. Zamanlama ve Durumu Manipüle Etme - (172)
8. Bilgi Toplama ve Analiz Etme - (118)
9. Erişim Kontrolünü Alt Üst Etme - (225)

Bu kategoriler, siber risklerin sistematik ve kapsamlı bir şekilde değerlendirilmesini sağlamakta ve ilgili hafifletme stratejilerinin geliştirilmesine yardımcı olmaktadır. Metodolojimiz, denizcilik sektöründe siber güvenlik önlemlerinin etkin bir şekilde uygulanmasını destekleyerek, operasyonel güvenliğin sağlanmasına yardımcı olmaktadır.

3.6 Monte Carlo Simülasyonu

Monte Carlo simülasyonu, bir projedeki belirsiz faktörlerin yerine bir dizi değer koyarak olası sonuçları modellemek için risk analizinde kullanılan güçlü bir olasılıksal matematiksel tekniktir (Joubert ve Pretorius, 2017). Bu yöntem, bir sistemin veya sürecin davranışını simüle etmek için çok sayıda rastgele örnek oluşturmayı içerir ve belirsizliğin proje üzerindeki etkisinin değerlendirilmesine olanak tanır. Monte Carlo simülasyonu, girdi değişkenleri için olasılık dağılımlarını birleştirerek potansiyel sonuçlara ve ilgili risklere ilişkin kapsamlı bir görünüm sağlar.

Monte Carlo simülasyonunun risk analizinde uygulanması finans, inşaat ve çevre bilimi dahil olmak üzere çeşitli alanlarda geniş çapta tanınmış ve incelenmiştir (Widodo vd., 2021). Riskleri değerlendirmek ve ölçmek için etkili bir araç olarak kabul edilir ve karar vericilerin bir projedeki belirsizlikleri anlamasını sağlar. Monte Carlo simülasyonu, risk modellerinin geliştirilmesine, risk parametrelerinin değerlendirilmesine ve belirlenen risklerin proje sonuçları üzerindeki etkisinin değerlendirilmesine yardımcı olur.

Monte Carlo simülasyonunun temel prensibi, bir modelin giriş değişkenleri için olasılık dağılımları belirlemek ve bu dağılımlardan rastgele değerler çekerek modelin çok sayıda simülasyonunu gerçekleştirmektir. Her bir simülasyon, modelin belirli bir dizi rastgele seçilmiş giriş değerine verdiği tepkiyi temsil eder ve bu tepkiler, projenin sonuçları üzerinde potansiyel bir dizi senaryo oluşturur. Bu şekilde, Monte Carlo simülasyonu, giriş değişkenlerindeki belirsizliklerin olası sonuçlar üzerindeki etkisini kapsamlı bir şekilde analiz eder.

Monte Carlo simülasyonunun matematiksel temeli, olasılık teorisi ve istatistiksel analiz üzerine kuruludur. Bir simülasyonun her bir adımında, modelin giriş değişkenlerinin olasılık dağılımlarından rastgele bir örnek seçilir. Bu işlem, her bir giriş değişkeni $\boldsymbol{Xi}$ için bir olasılık dağılımı $\boldsymbol{f(Xi)}$ ile tanımlanır. Giriş değişkenlerinin her biri için rastgele bir değer $\boldsymbol{x_i}$ seçildikten sonra bu değerler modele uygulanır ve modelin çıkış değeri $\boldsymbol{Y}$ hesaplanır. Bu süreç, aşağıdaki gibi ifade edilebilir:

$$\boldsymbol{Y = f(X1, X2, \dots, Xn)} \tag{3.1}$$

Burada $\boldsymbol{X1, X2, \dots, XnX1, X2, \dots, Xn}$ modelin giriş değişkenlerini, $\boldsymbol{f}$ ise bu değişkenlerin bir fonksiyonu olarak modelin çıktısını temsil etmektedir. Monte Carlo simülasyonu, bu süreci $\boldsymbol{N}$ kez tekrarlayarak, $\boldsymbol{Y}$ çıktısı için bir dağılım oluşturur. Sonuç olarak, elde edilen $\boldsymbol{Y}$ değerlerinin dağılımı, belirsizliğin ve riskin proje üzerindeki potansiyel etkilerini temsil eder.

Monte Carlo simülasyonunun uygulanmasında kullanılan teknikler arasında rasgele sayı üretimi ve rastgele örnekleme yer alır. Bu teknikler, giriş değişkenlerinin olasılık dağılımlarından doğru bir şekilde örnek alınmasını sağlar. Monte Carlo simülasyonu, karar vericilere, belirsizliğin ve riskin proje sonuçları üzerindeki etkisini daha iyi anlama ve yönetme olanağı sağlar.

Bu yöntem, risk modellerinin geliştirilmesine, risk parametrelerinin değerlendirilmesine ve belirlenen risklerin proje sonuçları üzerindeki etkisinin değerlendirilmesine yardımcı olur. Bu sayede, projelerde karşılaşılan belirsizlikler daha iyi yönetilebilir ve risklerin minimize edilmesi için daha etkin stratejiler geliştirilebilir. Bu durum, Monte Carlo simülasyonunu, belirsizliklerin yoğun olduğu projelerde vazgeçilmez bir araç haline getirmektedir.

3.7 Çarpan Etkisi Yaklaşımı

Çarpan etkisi yaklaşımı, ekonomik büyüme ve kalkınma süreçlerinde önemli bir rol oynamaktadır. Bu yaklaşım, bir ekonomik aktivitedeki artışın, diğer ekonomik faaliyetleri nasıl etkilediğini ve dolayısıyla toplam ekonomik büyümeyi nasıl artırdığını açıklamaktadır. Özellikle, kamu harcamaları, yatırımlar ve dış ticaret gibi unsurların çarpan etkisi ile ekonomik büyümeye katkıları üzerinde yoğunlaşılmaktadır.

Bu durum, bir başlangıç harcamasının, ekonomideki gelir ve harcamalarda bir dizi artışa yol açmasıyla açıklanır. Bu süreçte, ilk harcama bir dizi ikinci dereceden harcamayı tetikler, bu da ekonomik aktiviteyi daha da artırır. Çarpan etkisi, bu sürecin toplam etkisini ölçmek için kullanılır.

Türkiye'deki kalkınma planları çerçevesinde, güçlü yönetişim yapılarının oluşturulması ve kurumlara güvenin tesis edilmesi, çarpan etkisi ile gelişme sürecini hızlandıran unsurlar arasında yer almaktadır. Bu bağlamda, Türkiye'nin uzun vadeli ekonomik hedeflerine ulaşmasında çarpan etkisinin önemi giderek artmaktadır (Atakisi ve Cebeci, 2022). Ayrıca, sigorta sektörünün yarattığı dışsallıklar sayesinde ekonomik büyüme üzerindeki çarpan etkisi de dikkate değerdir. Sigorta sektörü, tasarruf ve finansman imkanları sağlayarak, gelişmekte olan Türkiye ekonomisinin yatırımlar için ihtiyaç duyduğu ortamı oluşturmaktadır (Özcan vd., 2021).

Dış ticaretin ekonomik büyüme üzerindeki etkisi de çarpan etkisi yaklaşımının bir başka örneğidir. Dış ticaret hacmindeki artışların, bazı ülkelerde ekonomik büyümeyi olumlu yönde etkileyebileceği, ancak her zaman bu etkinin sağlanamayabileceği vurgulanmaktadır (Demirel ve Işcan, 2021). Bu durum, çarpan etkisinin ülkelere göre değişiklik gösterdiğini ve ekonomik büyüme ile dış ticaret arasındaki ilişkinin karmaşık olduğunu göstermektedir.

Çarpan etkisinin temelinde, bir ekonomideki harcama, gelir ve üretim arasındaki ilişkiler yer alır. Bu etkilerin matematiksel olarak ifade edilmesi, çarpan katsayısının ($\boldsymbol{k}$) belirlenmesiyle yapılır. Çarpan katsayısı, marjinal tüketim eğilimi ($\boldsymbol{MPC}$) ve marjinal tasarruf eğilimi ($\boldsymbol{MPS}$) ile ilişkilidir.

Bu yöntem, risk modellerinin geliştirilmesine, risk parametrelerinin değerlendirilmesine ve belirlenen risklerin proje sonuçları üzerindeki etkisinin değerlendirilmesine yardımcı olur. Bu sayede, projelerde karşılaşılan belirsizlikler daha iyi yönetilebilir ve risklerin minimize edilmesi için daha etkin stratejiler geliştirilebilir. Bu durum, Monte Carlo simülasyonunu, belirsizliklerin yoğun olduğu projelerde vazgeçilmez bir araç haline getirmektedir.

$$\boldsymbol{k = 1 - MPC = MPS} \tag{3.2}$$

- $\boldsymbol{MPC}$ (Marjinal Tüketim Eğilimi): Gelirdeki her birim artışın tüketim harcamalarına ne kadarının yönlendirildiğini göstermektedir.

- $\boldsymbol{MPS}$ (Marjinal Tasarruf Eğilimi): Gelirdeki her birim artışın tasarrufa ne kadarının ayrıldığını göstermektedir.

Çarpan katsayısı $\boldsymbol{k}$, başlangıçtaki harcama değişikliğinin ekonomideki toplam gelir üzerindeki etkisini ölçer. Örneğin, hükümet harcamalarında $\boldsymbol{\Delta G}$ kadar bir artış olduğunda, bu artışın toplam gelir üzerindeki etkisi $\boldsymbol{k \times \Delta G k}$ olarak hesaplanır.

Çarpan etkisi, ekonomi politikalarının etkilerini değerlendirmede önemli bir araçtır ve harcama, gelir ve istihdam gibi makroekonomik değişkenlerin nasıl birbirleriyle etkileşime girdiğini analiz etmek için kullanılır.

3.8 Optimum Maliyet Dengesi

Optimum maliyet dengesi, ekonomik teoride, belirli bir üretim veya hizmet sunumu sürecinde maliyetlerin en düşük seviyeye çekilmesi ve kaynakların en verimli şekilde kullanılması amacıyla yapılan dengelemeleri ifade eder. Bu kavram, özellikle işletmelerin ve organizasyonların karar alma süreçlerinde önemli bir yer tutar. Optimum maliyet dengesi, genellikle maliyetlerin minimize edilmesi ile birlikte, elde edilen çıktının veya hizmetin kalitesinin artırılması hedefiyle ilişkilidir (Koç ve Güven, 2023).

Ekonomik teoride, optimum maliyet dengesi, genellikle Pareto optimalite kavramıyla ilişkilidir. Pareto optimalite, bir ekonomik durumun, bir bireyin durumunu kötüleştirmeden başka bir bireyin durumunu iyileştiremeyeceği bir durumu ifade eder. Bu bağlamda, optimum maliyet dengesi, kaynakların en verimli şekilde dağıtılması ve kullanılması için kritik bir öneme sahiptir (Dorta-González vd., 2002). Özellikle, maliyetlerin minimize edilmesi ve sosyal refahın artırılması hedefleri doğrultusunda, optimum maliyet dengesi sağlanmalıdır.

Ayrıca, optimum maliyet dengesi, çeşitli sektörlerde, özellikle de enerji yönetimi ve çevresel sürdürülebilirlik alanlarında da önemli bir kavramdır. Enerji sistemlerinin optimizasyonu, maliyetlerin düşürülmesi ve çevresel etkilerin azaltılması hedefleri doğrultusunda gerçekleştirilir. Bu tür sistemlerde, optimum maliyet dengesi sağlamak, hem ekonomik hem de çevresel sürdürülebilirlik açısından kritik bir öneme sahiptir (Güven vd Yörükeren, 2022).

Optimum Maliyet Dengesi, bir işletmenin belirli bir üretim seviyesinde veya projede en düşük maliyetle en yüksek verimliliği sağlamayı amaçlayan bir maliyet

yönetim stratejisidir. Bu kavram, üretim veya operasyon süreçlerinde hem sabit hem de değişken maliyetlerin dikkatli bir şekilde dengelenmesini içerir. Amaç, toplam maliyetleri minimize ederken, aynı zamanda kalite, üretim hacmi ve diğer performans kriterlerinden ödün vermemektir.

Optimum Maliyet Dengesi, genellikle marjinal maliyetler ve marjinal faydalar arasındaki dengeyi bulmaya dayanır. Marjinal maliyet, bir birim daha fazla üretim yapmanın getirdiği ek maliyeti ifade ederken, marjinal fayda, bu ek birim üretimin getirdiği ek geliri veya faydayı ifade eder. Optimum denge, marjinal maliyetin marjinal faydaya eşit olduğu noktada sağlanır. Optimum Maliyet Dengesi, matematiksel olarak $\boldsymbol{MC = MR}$ şeklinde gösterilmektedir:

$\boldsymbol{MC}$ = Marjinal Maliyet

$\boldsymbol{MR}$ = Marjinal Gelir

Bu denge noktası, bir işletmenin maliyetleri minimuma indirirken, üretimden elde ettiği gelir veya faydayı maksimuma çıkardığı durumu temsil eder. Optimum Maliyet Dengesi, maliyetleri kontrol altında tutarken, aynı zamanda işletmenin hedeflerine ulaşmasını sağlayacak kaynak tahsisini optimize etmeyi amaçlar. Bu kavram, işletme yönetimi, üretim planlaması, tedarik zinciri yönetimi ve proje yönetimi gibi birçok alanda uygulanabilir.

3.8.1 Optimum maliyet dengesi algoritması

Optimum Maliyet Dengesi Algoritması, bir işletmenin veya sistemin, belirli kısıtlar altında en düşük maliyetle en yüksek performansı veya verimliliği elde etmesini sağlayan bir optimizasyon algoritmasıdır. Bu algoritma, maliyetlerin minimize edilmesi ve performansın maksimize edilmesi arasında bir denge kurmayı amaçlar. Genellikle üretim, tedarik zinciri yönetimi, proje yönetimi ve kaynak tahsisi gibi alanlarda kullanılır.

Optimum Maliyet Dengesi Algoritması, maliyet fonksiyonları, kısıtlar ve hedefler belirlenerek uygulanır ve bu bileşenler üzerinden en uygun çözümün bulunmasına çalışılır. Algoritma, optimizasyon teorisi ve matematiksel programlama tekniklerine dayanır. Algoritmanın temel amacı, bir maliyet fonksiyonunu minimize ederken, belirli kısıtlar altında bir hedef fonksiyonunu maksimize etmektir.

Algoritmanın matematiksel temeli, bir objektif fonksiyonun $\boldsymbol{C(x)}$ maliyet fonksiyonunu temsil ettiği ve bu fonksiyonun minimize edilmek istendiği durumları kapsar. Fonksiyon genellikle şu şekilde ifade edilir:

$$\boldsymbol{minC(x) = \sum_{i=1}^{n} C_i \times x_i} \quad (3.3)$$

Formül içindeki ifadeler şu şekildedir:

- $\boldsymbol{C(x)}$ = Toplam maliyet fonksiyonu
- $\boldsymbol{C_i}$= Birim maliyet
- $\boldsymbol{x_i}$ = Karar değişkenleri (örneğin, üretim miktarı, hammadde kullanımı vb.)

Algoritmanın matematiksel temeli, bir objektif fonksiyonun $\boldsymbol{C(x)}$ maliyet fonksiyonunu temsil ettiği ve bu fonksiyonun minimize edilmek istendiği durumları kapsar. Fonksiyon genellikle şu şekilde ifade edilir:

- $\boldsymbol{g_j(x)}$= Kısıt fonksiyonları
- $\boldsymbol{b_j}$= Kısıtların sınır değerleri

$$\boldsymbol{g_j(x) \leq b_j \quad (j = 1, 2, \ldots, m)} \quad (3.4)$$

Bu denklemler kullanılarak, Optimum Maliyet Dengesi Algoritması, $\boldsymbol{x_i}$ karar değişkenlerinin hangi değerlerinin toplam maliyeti minimize ederken kısıtları ihlal etmeyeceğini bulur. Çözüm, doğrusal programlama teknikleri veya Newton-Raphson yöntemi gibi iteratif yöntemlerle elde edilebilir. Algoritmanın hedefi, hem maliyetleri azaltmak hem de performansı maksimize etmek için en uygun dengeyi bulmaktır.

4. BULGULAR VE TARTIŞMA

Bu çalışma, denizcilik sektöründe geçmişte yaşanan siber olayları analiz ederek, gemilerdeki bilgisayar destekli sistemleri hedef alan siber riskleri tespit etmeyi ve MITRE CAPEC ID'lerine dayalı Monte Carlo simülasyonunu kullanarak matematiksel bir risk analiz modeli geliştirmeyi amaçlamaktadır. Çalışmada, MITRE CAPEC çerçevesinin saldırı vektörlerini ve Çarpan Etkisi Yaklaşımını kullanarak, modern ticari gemilerin karşılaşması muhtemel siber tehditlerin potansiyel etkilerini formüle eden bir araştırma tasarımı kullanılmaktadır. Daha sonra bu riskler Monte Carlo simülasyonu yoluyla işlenerek matematiksel sonuçlar elde edilmektedir.

Literatür taraması için akademik veri tabanları araştırılarak denizcilik sektörüne özel siber saldırılar, karşı önlemler ve tehditler incelenmiştir. Ayrıca, geçmiş siber olayları analiz etmek için NHL Stenden Uygulamalı Bilimler Üniversitesi'nin Denizcilik Siber Saldırı Veritabanı (MCAD) kullanılmıştır. Gemilerdeki bilgisayar destekli sistemleri hedef alan tüm saldırı yöntemleri incelendi ve her bir bileşen için CAPEC saldırı vektörü, risk olasılığı, risk şiddeti ve risk etkisi işlenmiştir.

Çarpan Etkisi Yaklaşımı kullanılarak risk etkisi hesaplandıktan sonra CVSS 3.0'a dayalı olarak risklerin Düşük, Orta, Yüksek ve Çok Yüksek olarak kategorize edildiği bir Risk Skoru elde edilmiştir. Tüm analiz ve hesaplamalara dayanarak gemi bileşenlerine yönelik saldırı modeli olarak kullanılabilecek CAPEC'ler ve sonuçları bir tablo halinde sunulmaktadır. Denizcilik sektöründe yaşanan geçmiş siber olayların saldırı vektörleri incelenerek veriler elde edilmiştir.

Siber saldırılara maruz kalan gemi bileşenlerinin (varlıklarının) yazılım ve donanım açıkları da incelenerek çalışmanın bileşenleri ve CAPEC saldırı vektörleri için nihai veri seti oluşturuldu. Saldırı vektörleri ve bileşenleri değişken olarak ele alınmış ve bu değişkenlere uygulanabilecek koruyucu güvenlik önlemleri de çözüm olarak önerilmiştir. Elde edilen değişkenler ve değerlendirmeler Tablo 1'de sunulmaktadır.

Çizelge 4.1: Gemi Bileşenleri CAPEC ID'leri, Olasılık, Şiddet ve Etki Değerleri

Bileşen	CAPEC ID	Olasılık	Şiddet	Etki
AIS	CAPEC-28	Yüksek	Orta	Yüksek
	CAPEC-94	Yüksek	Çok Yüksek	Çok Yüksek
	CAPEC-117	Düşük	Orta	Orta
	CAPEC-151	Orta	Orta	Orta
	CAPEC-153	Orta	Orta	Orta
	CAPEC-184	Orta	Yüksek	Yüksek
	CAPEC-440	Düşük	Yüksek	Orta
	CAPEC-594	Orta	Yüksek	Yüksek
Anemometer	CAPEC-440	Düşük	Yüksek	Orta
	CAPEC-507	Düşük	Orta	Orta
BNWAS	CAPEC-122	Yüksek	Orta	Orta
	CAPEC-153	Orta	Orta	Orta
	CAPEC-390	Düşük	Yüksek	Orta
Central Alert Management HMI	CAPEC-122	Yüksek	Orta	Orta
	CAPEC-547	Düşük	Yüksek	Yüksek
Computers & Servers	CAPEC-2	Yüksek	Orta	Orta
	CAPEC-70	Orta	Yüksek	Orta
	CAPEC-122	Yüksek	Orta	Orta
	CAPEC-125	Yüksek	Orta	Orta
	CAPEC-441	Orta	Yüksek	Yüksek
	CAPEC-439	Düşük	Yüksek	Yüksek
	CAPEC-578	Orta	Orta	Orta
	CAPEC-593	Yüksek	Çok Yüksek	Yüksek
	CAPEC-600	Yüksek	Yüksek	Yüksek
	CAPEC-699	Orta	Yüksek	Yüksek
ECDIS	CAPEC-125	Yüksek	Orta	Orta
	CAPEC-148	Orta	Orta	Orta
	CAPEC-490	Yüksek	Orta	Orta
Echo Sounder	CAPEC-148	Orta	Orta	Orta
	CAPEC-216	Yüksek	Yüksek	Yüksek
	CAPEC-272	Orta	Yüksek	Yüksek
Global Positioning System (GPS)	CAPEC-601	Orta	Yüksek	Yüksek
	CAPEC-627	Düşük	Yüksek	Çok Yüksek
Global Maritime Distress and Safety System (GMDSS)	CAPEC-122	Yüksek	Orta	Yüksek
	CAPEC-125	Yüksek	Orta	Yüksek
	CAPEC-216	Yüksek	Yüksek	Yüksek
	CAPEC-547	Orta	Yüksek	Yüksek
Gyro-Compass	CAPEC-212	Orta	Orta	Orta
	CAPEC-216	Yüksek	Yüksek	Yüksek
Heading Control System (HCS)	CAPEC-153	Orta	Orta	Orta
	CAPEC-124	Orta	Yüksek	Yüksek
	CAPEC-624	Düşük	Yüksek	Yüksek
Indicators	CAPEC-153	Orta	Orta	Orta
	CAPEC-272	Orta	Orta	Orta
Magnetic Compass	CAPEC-124	Orta	Orta	Orta
Main Engine Controls	CAPEC-161	Orta	Yüksek	Çok Yüksek
	CAPEC-441	Orta	Yüksek	Çok Yüksek
	CAPEC-490	Yüksek	Orta	Orta
	CAPEC-547	Düşük	Yüksek	Yüksek
Multi Function Display(MFD)	CAPEC-148	Orta	Orta	Orta
	CAPEC-634	Düşük	Yüksek	Yüksek
NAVTEX	CAPEC-216	Yüksek	Yüksek	Yüksek
	CAPEC-490	Yüksek	Orta	Orta
	CAPEC-547	Düşük	Yüksek	Yüksek

Çizelge 4.1: (Devamı) Gemi Bileşenleri CAPEC ID'leri, Olasılık, Şiddet ve Etki Değerleri

Bileşen	CAPEC ID	Olasılık	Şiddet	Etki
RADAR	CAPEC-122	Yüksek	Orta	Yüksek
	CAPEC-125	Yüksek	Orta	Yüksek
	CAPEC-148	Orta	Orta	Orta
	CAPEC-699	Orta	Yüksek	Yüksek
Rate of Turn Indicator (ROTI)	CAPEC 161	Orta	Yüksek	Çok Yüksek
	CAPEC-547	Düşük	Yüksek	Yüksek
	CAPEC-582	Düşük	Yüksek	Yüksek
	CAPEC-603	Orta	Yüksek	Çok Yüksek
Rudder Pump Selector Switch	CAPEC-547	Düşük	Yüksek	Yüksek
Sound Reception System	CAPEC-153	Orta	Orta	Orta
	CAPEC-582	Düşük	Yüksek	Yüksek
	CAPEC-603	Orta	Yüksek	Yüksek
Speed and Distance Measuring Equipment (SDME)	CAPEC-148	Orta	Orta	Orta
	CAPEC-272	Orta	Yüksek	Orta
	CAPEC-627	Düşük	Yüksek	Orta
Steering Mode Selector Switch	CAPEC-547	Düşük	Yüksek	Yüksek
Thruster Controls	CAPEC-153	Orta	Orta	Orta
	CAPEC-547	Düşük	Yüksek	Orta
Track Control System (TCS)	CAPEC-153	Orta	Orta	Orta
Transmitting Heading Device (THD)	CAPEC-153	Orta	Orta	Orta
	CAPEC-272	Orta	Yüksek	Orta
Voyage Data Recorder (VDR)	CAPEC-153	Orta	Orta	Orta

Her bir MITRE CAPEC saldırı vektörü yeniden incelendi ve denizcilik sektöründeki gemi bileşenlerinin ve siber saldırı vektörlerinin güvenlik açıklarına ve zayıflıklarına göre metrikler yeniden hesaplandı. MITRE CAPEC, her bir bileşenle ilişkili potansiyel risklerin anlaşılması için bir referans görevi görür ve hesaplanan risk düzeylerine göre güvenlik önlemlerinin önceliklendirilmesine yardımcı olur.

Her bir CAPEC ID'sini anlamak, denizcilik sistemlerini etkileyebilecek çeşitli siber tehditleri doğru bir şekilde tanımlamak ve kategorize etmek için önemlidir. Her CAPEC ID'si, belirli bir saldırı modeline karşılık gelir ve siber saldırganlar tarafından kullanılan siber saldırılar için detaylı açıklama ve metodoloji bilgisi sunmaktadır.

Bu bilgiler, güvenlik uzmanlarının belirli tehditlere yönelik etkili hafifletme stratejileri tasarlaması ve uygulaması için oldukça değerlidir. Ayrıca siber risk analizlerinin etkin ve doğru bir şekilde yapılabilmesi için saldırı vektörlerinin ve alınabilecek güvenlik önlemlerinin adreslenmesi de siber güvenlik açısından önemlidir.

Çizelge 4.2: Saldırı Modeli Olarak Kullanılabilecek CAPEC ID'leri

CAPEC-2: Inducing Account Lockout	Bir saldırgan, birden fazla başarısız girişimden sonra hesapları kilitleyen parola sınırlama mekanizması gibi bir sistemin güvenlik özelliğini kullanarak bir DoS saldırısı başlatır ve bu mekanizmayı tetikleyerek meşru kullanıcıların hesaplarını kilitler.
CAPEC-28: Fuzzing	Bir saldırgan, sistem zayıflıklarını bulmak için bulanıklaştırmayı kullanır. Bulanıklaştırma, sisteme rastgele girdiler besleyerek yazılım güvenliğini test eder ve sistem hakkında herhangi bir önyargı veya varsayım olmaksızın arızaları tespit eder.
CAPEC-70: Try Common or Default Usernames and Passwords	Bir saldırgan yetkisiz erişim elde etmek için genel veya varsayılan kullanıcı adları ve parolalar kullanabilir. Buna boş parolalar, bilinen satıcı varsayılanları ve basit, yaygın olarak kullanılan parolalar dahildir.
CAPEC-74: Manipulating State	Bir saldırgan hedef yazılım tarafından tutulan durum bilgilerini manipüle eder veya donanımda bir durum geçişi başlatır. Başarılı olursa, hedef sistem tehlikeye atılmış durumu kullanarak çalışır ve bu da istenmeyen davranışa veya yürütmeye yol açar.
CAPEC-94: Adversary in the Middle (AiTM)	Bir saldırgan, işlem verilerini değiştirmek veya elde etmek için genellikle istemci ve sunucu olmak üzere iki bileşen arasındaki iletişimi kesintiye uğratır. Bu genellikle bileşenler arasındaki iletişim kanalında konumlanmayı içerir.
CAPEC-114: Authentication Abuse	Bir saldırgan, kimlik doğrulama mekanizmasındaki veya uygulamasındaki zayıflıkları istismar ederek bir uygulamaya, hizmete veya cihaza yetkisiz erişim elde eder. Belirli bir olay dizisi, saldırgana erişim izni vermesine neden olabilir.
CAPEC-115: Authentication Bypass	Bir saldırgan, yetkili bir kullanıcının ayrıcalıklarına sahip bir uygulamaya, hizmete veya cihaza erişmek için bir kimlik doğrulama mekanizmasını atlatır. Bu, saldırganın herhangi bir kimlik doğrulama sürecinden geçmeden korunan verilere erişmesine olanak tanır.
CAPEC-117: Interception	Bir saldırgan, hassas bilgileri toplamak veya daha fazla saldırıyı desteklemek için hedefe giden veya hedeften gelen veri akışlarını izler. Bu saldırı, ağ trafiğini ve radyo iletişimleri gibi diğer veri akışlarını koklamayı içerebilir.
CAPEC-122: Privilege Abuse	Bir saldırgan, sistemdeki zafiyetleri sömürerek, ayrıcalıklı olmayan hesaplara maruz kalan ayrıcalıklı kullanıcılara yönelik özellikleri kullanır. Hassas bilgilere ve işlevselliğe erişimi kontrol etmek, yalnızca yetkili kullanıcıların bu kaynaklara erişebilmesini sağlamak için önemlidir.
CAPEC-124: Shared Resource Manipulation	Bir saldırgan, davranışı etkilemek için uygulama havuzları veya donanım pin çoklaması gibi paylaşılan kaynakları kullanır. Paylaşılan bir kaynağı manipüle etmek, ona güvenen diğer uygulamaları veya iş parçacıklarını tehlikeye atabilir.
CAPEC-125: Flooding	Bir saldırgan, çok sayıda etkileşimi hızla başlatarak, hız sınırlayıcı zayıflıkları istismar ederek hedef kaynaklarını tüketir. Bu saldırı erişimi engeller ve operasyonel manipülasyondan ziyade istek hacmine güvenerek çökmelere neden olabilir.
CAPEC-148: Content Spoofing	Bir saldırgan, görünürdeki kaynağı değiştirmeden içeriği orijinalinden farklı olacak şekilde değiştirir. Buna web sayfaları, e-postalar ve dosya transferleri dahildir ve kötü amaçlı yazılım ifşasına, mali dolandırıcılığa, gizlilik ihlallerine ve diğer olumsuz sonuçlara yol açar.
CAPEC-151: Identity Spoofing	Kimlik sahteciliği, bir hedefe ulaşmak için başka bir varlığın kimliğini üstlenmeyi içerir. Bir saldırgan, kötü amaçlı faaliyetler yürütmek için farklı bir kaynaktan geliyormuş gibi görünen iletiler oluşturabilir veya çalınmış veya sahte kimlik doğrulama kimlik bilgilerini kullanabilir.
CAPEC-153: Input Data Manipulation	Bir saldırgan, bir girdi işleme arayüzüne veri biçimini, yapısını ve bileşimini kontrol ederek girdi doğrulama zayıflıklarından yararlanır. Saldırgan, standart dışı veya beklenmeyen girdi sağlayarak hedef sistemin güvenliğini olumsuz etkileyebilir.

Çizelge 4.2: (Devamı) Saldırı Modeli Olarak Kullanılabilecek CAPEC ID'leri

CAPEC-161: Infrastructure Manipulation	**Bir saldırgan, mesajları kendi sunucularına yönlendirmek için ağ yönlendirmesini manipüle eder. Yönlendirmeden habersiz olan kurbanlar, kimlik bilgileri gibi hassas bilgileri bilmeden paylaşır ve güvenli bir şekilde bağlandıklarını düşünürler.**
CAPEC-184: Software Integrity Attack	Bir saldırgan, kullanıcının, programın, sunucunun veya cihazın kodunu, veri yapılarını veya donanım yazılımını tehlikeye atan eylemler gerçekleştirmesine neden olan olayları tetikler ve hedefin bütünlüğünü değiştirerek güvenli olmayan bir durum yaratır.
CAPEC-212: Functionality Misuse	Bir saldırgan, sistem işlevselliğini istenmeyen şekillerde kullanarak zarar vermek için meşru bir uygulama yeteneğini kullanır. Bu genellikle bir özelliğin aşırı kullanılmasını veya yetkisiz, hassas verilere erişmek için tasarım kusurlarından yararlanılmasını içerir.
CAPEC-216: Communication Channel Manipulation	Bir saldırgan, güvenliğini tehlikeye atmak için bir iletişim kanalındaki ayarları veya parametreleri değiştirir; bu da potansiyel olarak bilgi ifşasına, iletişim akışından veri ekleme/çıkarmaya ve sistemin tehlikeye atılmasına yol açabilir.
CAPEC-231: Oversized Serialized Data Payloads	Bir saldırgan, veri işleme sırasında ayrıştırıcıya büyük boyutlu serileştirilmiş veri yükleri enjekte ederek sistem kaynaklarını tüketme ve keyfi kod yürütülmesine olanak sağlama gibi olumsuz etkilere neden olur.
CAPEC-240: Resource Injection	Bir saldırgan, kaynak tanımlayıcılarını manipüle ederek girdi doğrulama zayıflıklarından yararlanır ve istenmeyen kaynak değişikliği veya belirtimine olanak tanır. Bu durum, hedef sistemde yetkisiz erişime, veri bozulmasına veya diğer güvenlik ihlallerine neden olabilir.
CAPEC-272: Protocol Manipulation	Bir saldırgan, kimliğe bürünme, veri hırsızlığı, oturum denetimi veya diğer istismarlar gibi saldırılar gerçekleştirmek için bir iletişim protokolünü bozar. Bu saldırılar, geçersiz varsayımları, yanlış uygulamaları veya protokolün kendisindeki içsel güvenlik açıklarını hedefler.
CAPEC-390: Bypassing Physical Security	Tesisler, kilitler, elektronik kart giriş sistemleri ve alarmlar dahil olmak üzere katmanlı fiziksel güvenlik modelleri kullanır. Rastgele ihlalleri azaltmasına rağmen, bu yaklaşım, güvenlikten kaçınmaya, gözetime ve kilitleri atlatmaya odaklanan planlı saldırılara karşı daha az etkilidir.
CAPEC-438: Modification During Manufacture	Bir saldırgan, tedarik zincirine saldırmak için üretim sırasında bir teknolojiyi veya bileşeni değiştirir. Yazılımı, donanımı veya tasarımı değiştirebilirler. En büyük risk, kötü amaçlı donanım veya cihazlar üretmek için kasıtlı tasarım manipülasyonudur.
CAPEC-439: Manipulation During Distribution	Bir saldırgan dağıtım sırasında bir ürünün, yazılımın veya teknolojinin bütünlüğünü tehlikeye atar. Tehdit, ürünlerin çeşitli tedarikçiler ve entegratörler arasında geçişi sırasında entegrasyon veya paketleme sırasında kurcalamanın meydana gelebileceği birden fazla dağıtım aşamasından kaynaklanır.
CAPEC-440: Hardware Integrity Attack	Saldırgan, sistem bakım sürecindeki zayıflıkları istismar ederek, kurbanın bulunduğu konumdaki teknoloji, ürün veya bileşenlerde değişiklik veya yeni kurulumlar yaparak, sistemin konuşlandırıldığı sırada saldırı gerçekleştirmeyi amaçlar.
CAPEC-441: Malicious Logic Insertion	Bir saldırgan, sistemin iyi huylu bir bileşenine gizli kötü amaçlı mantık (kötü amaçlı yazılım) ekleyerek, tebrik kartları, resim çerçeveleri ve projektörler gibi cihazlardaki dijital depolama, Bluetooth ve Wi-Fi gibi yeni saldırı vektörlerini kullanır.
CAPEC-476: Signature Spoofing by Misrepresentation	Bir saldırgan, görünüşte geçerli bir imzaya sahip ancak sahte bir kimliğe sahip bir veri bloğu oluşturmak için kodu ayrıştırma veya görüntülemedeki zayıflıkları kullanır. Bu manipülasyon, alıcı yazılımın veya kullanıcının tehlikeye atıcı eylemler gerçekleştirmesine yol açabilir.
CAPEC-490: Amplification	Bir saldırgan, sahte bir kaynak adresiyle üçüncü taraf bir hizmete istekler göndererek bir yükseltme saldırısı gerçekleştirir ve hedef sunucuya büyük yanıtlar gönderir; önemli miktarda trafik oluşturmak için asgari kaynakları kullanır.

Çizelge 4.2: (Devamı) Saldırı Modeli Olarak Kullanılabilecek CAPEC ID'leri

CAPEC-536: Data Injected During Configuration	**Bir saldırgan, kurbanın sisteminde yapılandırma veya yeniden ayarlama sırasında kritik operasyonel dosyalara kötü amaçlı veriler enjekte eder. Bu, sistemin yetersiz performans göstermesine neden olur, saldırgana fayda sağlar ve sistemin verimliliğini tehlikeye atar.**
CAPEC-547: Physical Destruction of Device or Component	Bir saldırgan bir cihaza veya bileşene fiziksel olarak saldırır ve onu işlevsiz hale getirir. Bu yıkım, cihazın amaçlandığı gibi çalışmasını engeller, normal işlevini bozar ve potansiyel olarak önemli bir operasyonel etkiye neden olur.
CAPEC-578: Disable Security Software	Bir saldırgan, algılamanın gerçekleşmemesi için güvenlik araçlarını devre dışı bırakmak amacıyla erişim kontrolündeki bir zayıflıktan yararlanır. Bu, işlemleri öldürme, kayıt defteri anahtarlarını silme, böylece araçların çalışma zamanında başlamaması, günlük dosyalarını silme veya diğer yöntemler şeklinde olabilir.
CAPEC-582: Route Disabling	Bir saldırgan, iki hedef arasındaki ağ rotasını devre dışı bırakarak iletişim kanallarını keser. Bu, veriyi değil rotanın kendisini hedef alması nedeniyle tipik engelleme saldırılarından farklıdır. Büyük hatalardan veya altyapı kontrolünden kaynaklanabilir.
CAPEC-593: Session Hijacking	Bu tür saldırı, kimlik doğrulaması gerçekleştirirken bir uygulamanın oturum kullanımındaki zayıflıkları istismar eden bir saldırganı içerir. Saldırgan, etkin bir oturumu çalabilir veya manipüle edebilir ve bunu uygulamaya yetkisiz erişim elde etmek için kullanabilir.
CAPEC-594: Traffic Injection	Bir saldırgan, hedefin ağ bağlantısını bozmak veya kesintiye uğratmak ve potansiyel olarak içeriği değiştirmek için ona trafik enjekte eder. Bu hedefli saldırı, kaynakları su basması yoluyla tüketmek yerine, sistemi etkilemek için belirli girdiler oluşturur.
CAPEC-600: Credential Stuffing	Bir saldırgan, erişim elde etmek için birden fazla sistemde bilinen kullanıcı adı/şifre kombinasyonlarını kullanır. Kimlik bilgisi doldurma, kullanıcıların kimlik bilgilerini tekrar kullanma alışkanlığını istismar ederek başarılı yetkisiz erişim şansını artırır.
CAPEC-601: Jamming	Bir saldırgan, iletişimi bozmak için radyo gürültüsünü veya sinyallerini kullanır. Sistem kaynaklarını yasa dışı trafikle bilerek boğmak suretiyle, yetkili kullanıcıların meşru trafiğine hizmet reddedilir.
CAPEC-603: Blockage	Bir saldırgan kritik bir sistem kaynağının teslimatını engeller ve sistemin arızalanmasına veya işlevinin durmasına neden olur. Bu kesinti, operasyonları durdurabilir ve önemli bir kesintiye ve sistemin bütünlüğüne potansiyel zarara yol açabilir.
CAPEC-624: Hardware Fault Injection	Saldırgan, elektromanyetik darbeler, lazer darbeleri ve aşırı sıcaklıklar gibi bozucu sinyalleri veya çevresel değişiklikleri kullanarak cihaz arızalarına neden olabilir ve gizli anahtar bilgilerini elde etmek için şifreleme işlemlerini suistimal edebilir.
CAPEC-627: Counterfeit GPS Signals	Bir saldırgan, normal sinyalleri taklit eden sahte GPS sinyalleri yayınlayarak bir GPS alıcısını aldatır. Bu sahte sinyaller, alıcının konumunu yanlış tahmin etmesine veya yanlış bir zaman kaydetmesine neden olur.
CAPEC-634: Probe Audio and Video Peripherals	Saldırgan, kötü amaçlı yazılım veya zamanlanmış görevler kullanarak ses ve video işlevlerini istismar eder, finansal, kişisel veya politik kazanç sağlamak amacıyla mikrofonlar, web kameraları veya ses ve video yeteneklerine sahip uygulamalar aracılığıyla hassas bilgileri ele geçirir.
CAPEC-699: Eavesdropping on a Monitor	Bir saldırgan, kablolar veya video portları tarafından yayılan sinyalleri yakalayarak harici bir monitörün içeriğini dinler, kabloları değiştirmeden veya yazılım yüklemeden veri gizliliğini etkiler ve geleneksel güvenlik uygulamaları/araçları tarafından tespit edilmekten kaçınır.

Risk hesaplama modelimiz olasılık, ciddiyet ve etki ölçümlerini tanımlamayı ve ardından bu ölçümleri listedeki her CAPED ID'ye göre bir risk puanına dönüştürmeyi içerir. Risk skorunu etkileyen faktörler aşağıda şu şekilde sıralanabilir:

- **Olasılık:** Bir saldırının gerçekleşme olasılığını ifade eder.
- **Saldırı Yüzeyi:** Ağın ne kadar açık ve savunmasız olduğunu ifade eder.
- **Düşman Beceri Seviyesi:** Saldırı için gereken teknik uzmanlığı belirtir.
- **Savunma Tedbirleri:** Saldırıyı önleyebilecek veya tespit edebilecek mevcut güvenlik kontrollerini ifade eder.
- **Yaygınlık:** Bu tür saldırıların benzer bağlamlarda ne kadar yaygın olduğunu gösterir.
- **Şiddet:** Saldırının neden olabileceği hasar veya aksamanın boyutunu ifade eder.

Etkiyi hesaplamak için Ağırlıklı Toplam Yaklaşımını veya Çarpan Etkisi Yaklaşımını kullanabiliriz. Çerçevemizde etkiyi daha kesin hesaplamak için Çarpan Etkisi Yaklaşımını kullanılmıştır. I = Etki (Impact), L = Olasılık (Likelihood) ve S = Seviye (Severity) ifade etmek üzere:

$$\boldsymbol{I = \sqrt{L \times S}} \tag{4.1}$$

Değerlendirilen her bir bileşen için olasılık, şiddet ve etki değerleri, bileşenlere yönelik potansiyel saldırı modeli görevi görebilecek CAPEC kimliklerinin yanı sıra siber güvenlik alanındaki kişisel gözlem ve değerlendirmelere göre belirlendi. Risk etkisi hesaplandıktan sonra Olasılık, Şiddet ve Etki çarpılarak Risk Puanını (RS) hesaplamak mümkündür. Risk Puanı aşağıdaki formülle hesaplanabilir:

$$\boldsymbol{RS = L \times S \times I} \tag{4.2}$$

Her bir bileşenin olasılık, şiddet ve etki değerleri, bileşenler için potansiyel saldırı modeli görevi görebilecek CAPEC ID'lerin yanı sıra siber güvenlik alanındaki kişisel gözlem ve değerlendirmelere göre belirlendi. CAPEC ID'ler Olasılık, Şiddet ve Etki puanlarını verse de, risk analizi modelimiz, azaltımları ve denizcilik teknolojisini, özellikle de gemi ICT'lerini ekleyerek farklı bir yaklaşım sunmaktadır.

Çizelge 4.3: Değerlendirme Puanları ve Tanımlar

Olasılık (L)	Derece (S)	Etki (I)	Risk Score (RS)
1 (Olası Değil)	1 (Önemsiz)	1 (İhmal Edilebilir)	*RS = L x S x I*
2 (Nadir)	2 (Küçük)	2 (Düşük)	*RS = L x S x I*
3 (Muhtemel)	3 (Orta)	3 (Orta)	*RS = L x S x I*
4 (Olası)	4 (Büyük)	4 (Yüksek)	*RS = L x S x I*
5 (Neredeyse Kesin)	5 (Felaket)	5 (Kritik)	*RS = L x S x I*

Dört risk seviyesinden oluşan bir risk puanlama tablosu oluşturduk: Düşük, Orta, Yüksek ve Kritik. Hesaplanan RS değerini Tablo 3'teki RS Aralığı ile eşleştirerek her bir potansiyel risk için Risk Düzeyini bulmak mümkündür. Deniz araçlarının operasyonel bütünlüğünü, güvenliğini ve verimliliğini korumak için riskin azaltılması esastır.

Kuruluşlar, riskleri azaltmaya yönelik stratejileri belirleyerek, değerlendirerek ve uygulayarak olası felaketleri, mali kayıpları ve operasyonel aksaklıkları önleyebilir. Etkin risk azaltma, uluslararası denizcilik düzenlemelerine uyumu sağlar, geminin sertifikasyonunu korur ve yasal yansımalardan kaçınır. Ek olarak, gemi operasyonlarının dayanıklılığını artırarak kritik sistemlerin olumsuz koşullarda veya siber tehditlerde bile işlevsel kalmasını sağlar.

Ayrıca gemi bileşenlerindeki her risk için matematiksel hesaplama eklemek amacıyla Monte Carlo simülasyonunu da kullandık. Monte Carlo simülasyonu, çok sayıda rastgele değişken örneğini kullanarak matematik problemlerini çözmek için kullanılan bir tekniktir. Bu yöntem özellikle belirsizliklerin ve değişkenlerin karmaşık olduğu durumlarda risk değerlendirmesi için kullanışlıdır.

Monte Carlo Simülasyonunu geliştirdiğimiz siber risk analizi modelimize dahil etmek için aşağıdaki adımlar uygulanabilir:

- **Olasılık Dağılımlarının Tanımlanması:** Her bir bileşen için olasılık, şiddet ve etki değerlerine ilişkin olasılık dağılımları tanımlanır. Bu dağılımlar tarihsel verilere ve uzman görüşlerine göre belirlenmektedir.
- **Rastgele Örnekler Oluşturma:** Tanımlanan olasılık dağılımlarından rastgele örnekler (örnek kümeleri) oluşturulur. Her örnek, belirli bir senaryo için olasılık, olasılık, şiddet ve etki değerlerini temsil eder.

- **Risk Puanlarının Hesaplanması:** Her numune için bir risk puanı hesaplanır. Risk puanlarının dağılımını elde etmek için bu hesaplamalar belirli bir dönemde binlerce kez tekrarlanır.
- **Sonuçların Analizi:** Elde edilen risk puanlarının dağılımı analiz edilir. Bu analiz, riskin ortalama değeri, varyans ve belirli bir eşiği aşma olasılığı gibi önemli istatistiksel ölçümleri içerir.
- **Karar Verme:** Analiz sonuçlarına göre en kritik bileşenler ve bunlar için alınması gereken önlemler belirlenir.

Her bileşen için olasılık dağılımları normal, log-normal, beta veya diğer uygun dağılımlar kullanılarak tanımlanır. Daha sonra her bir bileşen için Risk Puanı hesaplanır ve ardından Simülasyon Sonuçları Analizi için Ortalama Risk Puanı ve Varyans hesaplanır.

Öncelikle risk fonksiyonları oluşturulur. Her bileşen için CAPEC modeli içinde yer alan riskler aşağıdaki fonksiyonlardan geçirilir.

$$\boldsymbol{P(L) = f(L), P(S) = g(S), P(I) = h(I)} \tag{4.3}$$

- $\boldsymbol{L}$ = Bir olayın meydana gelme olasılığını veya sıklığını temsil eder.
- $\boldsymbol{S}$ = Olayın şiddetini veya etkisini temsil eder.
- $\boldsymbol{I}$ = Olayın etkisini temsil eder.

Formül içinde yer alan $\boldsymbol{L}$, $\boldsymbol{S}$ ve $\boldsymbol{I}$ faktörleri sırasıyla $\boldsymbol{f}()$, $\boldsymbol{g}()$ ve $\boldsymbol{h}()$ fonksiyonları aracılığıyla riskin olasılığına eşlenir.

Daha sonra risk envanteri içinde yer alan her bileşen için Risk Puanı (Risk Score) oluşturulur. Bunun için aşağıdaki formül kullanılmaktadır:

$$\boldsymbol{\left(i = 1, 2, \ldots, N\right) \; için \; RS_i = L_i \times S_i \times I_i} \tag{4.4}$$

Bu formül, $\boldsymbol{i}$'nci senaryo veya bileşen için Risk Puanı **RSi** 'yi hesaplar. Risk puanı, her senaryo veya bileşen $\boldsymbol{i}$ için olasılık $\boldsymbol{L_i}$, $\boldsymbol{S_i}$SiSi ve etki $\boldsymbol{I_i}$'nin çarpılmasıyla hesaplanır.

Daha sonra, tüm $\boldsymbol{N}$ senaryoları veya bileşenleri genelinde ortalama risk puanı $\boldsymbol{\mu RS}$ hesaplanır. Bireysel risk puanları $\boldsymbol{RS_i}$'nin aritmetik ortalamasıdır. $\sum_{\boldsymbol{i=1}}^{\boldsymbol{N}} \boldsymbol{RS_i}$i

toplamı tüm risk puanlarını toplar ve ardından elde edilen toplam değer, ortalamayı elde etmek için senaryo/bileşen sayısı olan $\boldsymbol{N}$'ye bölünür.

$$\boldsymbol{\mu RS} = \frac{\mathbf{1}}{\boldsymbol{N}} \sum_{\boldsymbol{i=1}}^{\boldsymbol{N}} \boldsymbol{RS_i} \tag{4.5}$$

Son olarak; risk puanlarının, ortalama risk puanı ($\boldsymbol{\mu RS}$) etrafındaki yayılımını veya değişkenliğini ölçen risk puanlarının varyansı $\boldsymbol{\sigma^2_{RS}}$ hesaplanır. Varyans, her risk puanı $\boldsymbol{RS_i}$ ile ortalama risk puanı $\boldsymbol{\mu RS}$ arasındaki farkın karesi alınarak ve ardından bu karelenmiş farkların tüm $\boldsymbol{N}$ senaryoları/bileşenleri arasında ortalamasının alınmasıyla hesaplanır.

$$\boldsymbol{\sigma^2_{RS}} = \frac{\mathbf{1}}{\boldsymbol{N}} \sum_{\boldsymbol{i=1}}^{\boldsymbol{N}} (\boldsymbol{RS_i} - \boldsymbol{\mu RS})^{\mathbf{2}} \tag{4.6}$$

Tanımlanan her risk için Başlangıç Risk Puanı (IRS) belirlendikten sonra, hedeflenen hafifletme çalışmaları gerçekleştirilir. Bu çabalar, maruz kalınan genel riskin yönetilmesi ve azaltılması açısından kritik öneme sahiptir. Süreç, önleyici faaliyetlerin tanımlanması ve uygulanması, ilgili maliyetlerin değerlendirilmesi, azaltılan risk oranının hesaplanması ve kalan etkinin değerlendirilmesi dahil olmak üzere birçok temel adımı içerir.

IRS hesaplandıktan sonra, belirlenen riskleri ele almak için özel hafifletme stratejileri geliştirilir ve uygulanır. Bu stratejiler, her bir riskin olasılığını, ciddiyetini ve etkisini azaltacak şekilde uyarlanmıştır. Önleyici faaliyetler teknolojik yükseltmeleri, süreç iyileştirmelerini, eğitim programlarını, politika değişikliklerini veya riski azaltmak için tasarlanmış diğer ilgili müdahaleleri içerebilir.

Her önleyici faaliyetin, değerlendirilmesi ve belgelenmesi gereken belirli bir maliyeti vardır. Bu, yeni teknolojinin satın alınması veya yeni süreçlerin uygulanması gibi doğrudan maliyetleri ve uygulama aşamasında personelin eğitimi veya olası kesintiler gibi dolaylı maliyetleri içerir. Azaltma çabalarının faydalarının ilgili maliyetlerden daha ağır basmasını sağlamak için kapsamlı bir maliyet-fayda analizi yapılır.

Önleyici faaliyetler sonucunda azaltılan riskin oranı hesaplanır. Bu genellikle yüzde olarak ifade edilir ve başlangıçtaki riskin ne kadarının etkili bir şekilde azaltıldığını gösterir. $\boldsymbol{PRM}$ = (Azaltılan Risk Miktarı) Proportion of Risk Mitigated, $\boldsymbol{MRS}$ = Azaltılmış Risk Puanı (Mitigated Risk Score), $\boldsymbol{IRS}$ = Başlangıç Risk Puanı

(Initial Risk Score), $\boldsymbol{RRS}$ = Artık Risk Puanı (Residual Risk Score) ve $\boldsymbol{C_{RI}}$ = Riskin Artık Maliyet Katsayısı (Cost of Residual Impact) ifade edilmek üzere;

$$\boldsymbol{PRM} = \frac{\boldsymbol{Azaltılan\ Riskin\ Yuzdesi}}{\boldsymbol{100}} \tag{4.7}$$

Azaltılmış risk, başlangıçtaki riski azaltmak için önleyici tedbirlerin ve hafifletme stratejilerinin uygulanmasından sonra kalan risk seviyesini ifade eder. Temel olarak, çeşitli risk yönetimi faaliyetleri yoluyla ele alınan ve en aza indirilen ilk riskin kısmıdır. Azaltma çabaları, risk olayının meydana gelme olasılığını azaltmayı, sonuçlarının ciddiyetini azaltmayı veya kuruluş üzerindeki genel etkisini azaltmayı amaçlamaktadır.

$$\boldsymbol{MRS(i) = IRS(i) \times PRM(i)} \tag{4.8}$$

Daha sonra kalan etki veya önleyici faaliyetlerin uygulanmasından sonra kalan risk değerlendirilir. Artık etki, olası tüm hafifletme önlemlerinin uygulanmasından sonra kalan risk düzeyini ifade eder. Başlangıçtaki riski azaltma veya kontrol etme çabalarına rağmen hala meydana gelebilecek potansiyel etki veya hasardır.

$$\boldsymbol{RRS(i) = IRS(i) - MRS(i)} \tag{4.9}$$

Artık Risk Puanı, kuruluşun sürekli olarak yönetmesi ve izlemesi gereken kalan riskin anlaşılmasına yardımcı olur. Son olarak, hem önleyici faaliyetlerin maliyetlerini hem de artık riskle ilişkili potansiyel maliyetleri içeren toplam azaltma maliyeti belirlenir. Toplam Maliyet (C_{total}) aşağıdaki formülle:

$$\boldsymbol{C_{total}} = \sum_{\boldsymbol{i-1}}^{\boldsymbol{n}} \left(\boldsymbol{Cost(i) + C_{RI}(i) \times RRS(i)}\right) \tag{4.10}$$

Bu kapsamlı değerlendirme, azaltma stratejilerinin yalnızca riski azaltmada etkili olmasını değil, aynı zamanda maliyet açısından da verimli olmasını sağlar. Kuruluşlar, bu stratejileri sürekli olarak değerlendirip geliştirerek risk yönetimi çerçevelerini geliştirebilir ve potansiyel tehditleri azaltmaya yönelik sağlam bir yaklaşım sağlayabilirler. Önleyici Tedbir Maliyeti belirlendikten sonra Toplam Maliyetin hesaplanması önemlidir.

Son adım, bir risk envanteri oluşturmak ve hafifletmek için bir bütçe tanımlamaktır. Daha sonra riskler bütçeye, başlangıç risk puanına, başlangıç maliyetine, azaltma maliyetine ve azaltma oranına göre önceliklendirilir. Optimum Maliyet Dengesi algoritması, önceden tanımlanmış bir bütçe dahilinde en uygun maliyetli önlemleri seçerek siber güvenlik riskini en aza indirmek için kullanılır. Aşağıdaki döngü, maliyetleri kalan bütçeyi aşmadığı sürece önlemleri yinelemeli olarak seçmektedir.

$$M_i = \frac{R_i}{C_i} \; for \; i = 1,2,...,N$$

$$Sort \; (M_i, i) \; in \; decending \; order \; by \; Mi$$

Initialize P = 0, Budget remaining = B

For each measure (M_i, i) *in sorted order:*

if $C_i \leq$ *Budget remaining:*

$P = P \cup \{i\}$

Budget remaining = Budget remaining – C_i

Bu bölümde Monte Carlo simülasyonuna dayalı risk analizi modelimiz kullanılarak elde edilen bulgular sunulmaktadır. Senaryo, denizcilik sektöründeki belirli bir gemi bileşeni için siber risklerin değerlendirilmesini içeriyor. Simülasyon sonuçları, gemi navigasyon sisteminin belirli senaryolar altında taşıdığı riskin düzeyini ve bu riski etkileyen faktörleri ortaya koymaktadır.

Monte Carlo simülasyon sonuçlarına göre etki büyüklüğü, belirli güvenlik önlemlerinin risk puanlarını nasıl değiştirebileceğini gösteriyor. Ortalama risk puanı ve varyansı kullanarak riskin ciddiyetini belirlemek önemlidir. CVSS skorlama sistemi uygun olsa da modelimiz için Risk Skoru Aralığımızı oluşturduk. Başlangıçta risk puanlarının belirli aralıklara göre sınıflandırılması gerekir:

Çizelge 4.4: Risk Seviyeleri ve Tanımları

RS Aralığı	Risk Seviyesi	Tanım
0.00 – 0.20	Düşük	Minimal risk, standart kontrollerle yönetilebilir.
0.21 – 0.40	Orta	Orta düzeyde risk, hedefli kontroller gerektirir.
0.41 – 0.60	Yüksek	Önemli risk, acil eylem gerektirir.
0.61 – 1.00	Çok Yüksek	Ciddi risk, acil ve kapsamlı eylem gerektirir.

Risk analizi için Monte Carlo simülasyonunu entegre etmek amacıyla **Python** programlama dili kullanılarak özel bir yazılım geliştirildi. Yazılım, istatistiksel veri analizi için güçlü **numpy** paketinden ve histogramlar oluşturmak için **matplotlib** paketinden yararlanır. Bu yazılım, bir sistemin çeşitli bileşenleriyle, bu durumda bir gemi bileşeniyle ilişkili riski değerlendirmeyi amaçlamaktadır. Yazılım, Monte Carlo simülasyonunu kullanarak, risk değerlendirme parametrelerindeki doğal belirsizlikleri hesaba katan olasılıksal bir analiz sağlar.

Bu parametrelerin her biri için, tahminlerdeki belirsizlikleri hesaba katmak amacıyla tahmini standart sapma değerleri kullanılır. Monte Carlo simülasyonu, bu standart sapmalarla tanımlanan olasılık dağılımlarından örnekleme yaparak çok sayıda senaryo üretir ve potansiyel sonuçlara ilişkin kapsamlı bir görünüm sağlar. Simülasyonun ardından yazılım, oluşturulan risk puanlarından aşağıdaki istatistiksel ölçümleri hesaplar.

Risk analizinin sonuçları, risk puanlarının dağılımının grafiksel bir temsilini sağlayan histogramlar kullanılarak görselleştirilir. Bu görselleştirme, risk ölçümlerinin anlaşılmasına yardımcı olur. Seçilen bir gemi bileşeni için simülasyon sonuçları aşağıdaki gibidir:

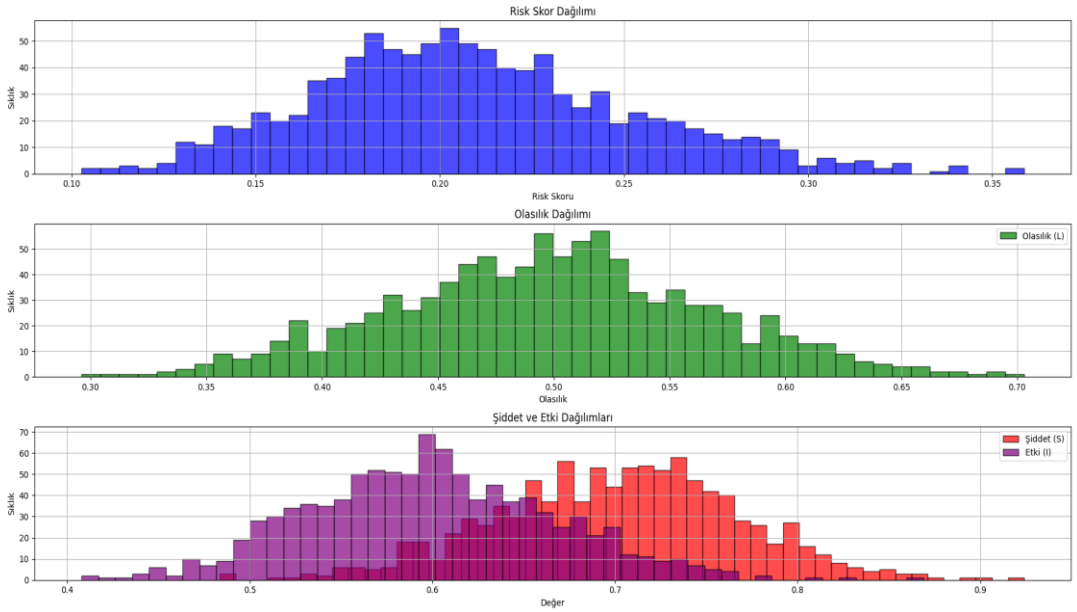
- **Mean Risk Score (μ_{RS}):** 0.20801597849455428
- **Risk Score Variance (σ^2_{RS}):** 0.0015108564402906298
- **Risk Severity:** Very High
- **Risk Probability (L_{mean}):** 0.5
- **Risk Severity (S_{mean}):** 0.7
- **Risk Impact (I_{mean}):** 0.6000000000000001

Tüm sistemin genel risk puanını doğru bir şekilde belirlemek ve şirketin güvenlik durumunu değerlendirmek için her bir riskin sistematik, yinelenen bir süreç yoluyla hesaplanması önemlidir. Bu, her biri için Monte Carlo simülasyonunu kullanarak sistem içindeki tüm bileşenleri veya risk faktörlerini metodik olarak değerlendiren bir döngünün yürütülmesini içerir.

Yinelemeli döngü, simülasyonun çeşitli risk faktörleri arasındaki karmaşık etkileşimleri ve bağımlılıkları yakalamasını sağlar. Simülasyon çalışırken, sistemin risk ortamına ilişkin kapsamlı ve bütünsel bir görünüm sağlamak için bireysel risk puanlarını bir araya getirir. Bu toplu risk profili, karar vericilerin risk hafifletme ve

yönetimine ilişkin iyi bilgilendirilmiş, stratejik kararlar almasına olanak sağlamada etkilidir.

Kuruluşlar, kümülatif riski anlayarak çabalarını önceliklendirebilir ve en önemli güvenlik açıklarını gidermek için kaynakları etkili bir şekilde tahsis edebilir. Bu yaklaşım, yalnızca genel siber güvenlik direncini artırmakla kalmıyor, aynı zamanda mevcut bütçenin risk azaltımını en üst düzeye çıkaracak şekilde kullanılmasını sağlayarak şirketin potansiyel siber tehditlere karşı savunma duruşunu güçlendiriyor.



Şekil 4.1: Risk Şiddeti ve Etkisi Dağılım Histogramı

Araç, belirli bir bütçeye göre siber güvenlik önlemlerinin seçimini optimize etmek için sistematik bir yaklaşım kullanıyor. Risk ve maliyet analizi yapar, önlemleri önceliklendirir ve mevcut bütçe dahilinde riskleri azaltmak için en uygun maliyetli çözümleri üretir. Araç aynı zamanda siber güvenlik önlemlerini değerlendirmek ve önceliklendirmek için Optimum Maliyet Dengesi Algoritmasını da kullanıyor. Süreçte yer alan temel adımlar şunlardır:

1. **Risk ve Maliyet Veri Girişi:** Kullanıcı, çeşitli siber güvenlik önlemleri için maliyetler, risk azaltımları, başlangıç risk puanları ve başlangıç risk maliyetleri dahil olmak üzere gerekli verileri sağlar. Ayrıca toplam bütçe de belirtilir.

2. **Verimlilik Oranlarının Hesaplanması:** Araç, her önlem için birim maliyet başına risk azaltımı olarak tanımlanan verimlilik oranını hesaplar. Bu oran, her önlemin maliyet etkinliğinin belirlenmesine yardımcı olur.
3. **Tedbirlerin Sıralanması:** Tedbirler, etkinlik oranlarına göre azalan düzende sıralanarak en etkili tedbirlerin ilk önce dikkate alınması sağlanır.
4. **Bütçe Kısıtlı Seçim:** Araç, sıralanan listeyi yineler ve sağlanan bütçe dahilinde uygulanabilecek önlemleri seçer. Kalan bütçeyi takip eder ve başka önlem alınamadığında durur.

Araç, başlangıç risk puanı, başlangıç risk maliyeti, risk azaltma ve azaltma maliyeti de dahil olmak üzere her riskin ayrıntılarını belgelemektedir. Bu kapsamlı bilgi, mevcut durum koşullarını anlamak ve her bir hafifletme önleminin potansiyel etkisini değerlendirmek için çok önemlidir. Araç, ayrıntılı dokümantasyonun yanı sıra, her bir risk için hafifletme maliyetlerinin ve başlangıç risk maliyetlerinin grafik biçiminde görsel bir temsilini de oluşturmaktadır.

Bu görsel yardım, maliyet dağılımını ve her bir önlemin göreceli etkisini göstermede etkilidir. Grafik, risk yönetiminin finansal yönlerini açıkça göstererek karar vericilerin farklı riskleri ve bunlarla ilişkili maliyetleri hızlı bir şekilde karşılaştırmasına ve karşılaştırmasına yardımcı olarak, risk azaltımını en üst düzeye çıkarmak için kaynakların en etkili şekilde nereye tahsis edilebileceğinin daha derinlemesine anlaşılmasını kolaylaştırmaktadır.

Çizelge 4.5: Risk Azaltma Oranları ve Azaltma Maliyetleri (Toplam Bütçe=15000$)

Risk ID	İlk RS	İlk RC ($k)	Risk Azaltma (%)	Önlem Maliyeti ($k)
01	7.8	5000	45.8	2500
02	8.5	6500	55.4	2000
03	8.1	5500	61.3	1500
04	7.5	6000	51.6	2500
05	6.8	7500	25.2	3000
06	5.5	4500	33.5	1000
07	7.3	3000	40.7	2200
08	6.2	7000	66.1	3500
09	8.8	3500	50.4	1800
10	9.3	4000	46.9	2000

Araç, belirli bir bütçe dahilinde en yüksek risk azaltımını sağlayan siber güvenlik önlemlerini etkili bir şekilde önceliklendirip, seçmektedir. Kantitatif analizi

görselleştirmeyle birleştirerek karar vericilerin en kritik riskleri etkili bir şekilde anlamalarına ve ele almalarına yardımcı olmaktadır.

Seçilen önlemler, mevcut kaynakların en etkili şekilde kullanılmasını sağlayarak şirketin güvenlik duruşunu geliştirmeye yönelik stratejik bir yaklaşımı temsil etmektedir. Araç, bütçe kısıtlamalarına ve verimlilik oranlarına göre siber güvenlik önlemlerini seçmektedir.

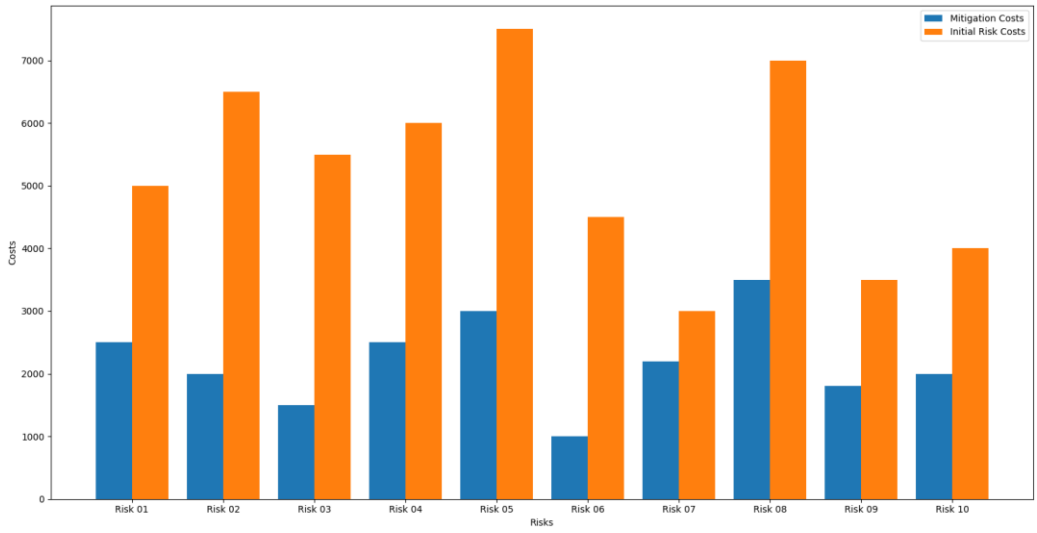
```
TOTAL BUDGET = 15000

Risk Details:
Risk | Initial Risk Score | Initial Risk Cost | Risk Reduction | Mitigation Cost
-------------------------------------------------------------------------------
 01  |      7.8           |      5000         |     45.8       |     2500
 02  |      8.5           |      6500         |     55.4       |     2000
 03  |      8.1           |      5500         |     61.3       |     1500
 04  |      7.5           |      6000         |     51.0       |     2500
 05  |      6.8           |      7500         |     25.0       |     3000
 06  |      5.5           |      4500         |     33.5       |     1000
 07  |      7.3           |      3000         |     40.2       |     2200
 08  |      6.2           |      7000         |     66.1       |     3500
 09  |      8.8           |      3500         |     50.7       |     1800
 10  |      9.3           |      4000         |     45.4       |     2000

Selected Cybersecurity Measures:
  Risk 03
  Risk 06
  Risk 09
  Risk 02
  Risk 10
  Risk 04
  Risk 08
```

Şekil 4.2: Seçilen Koruyucu Siber Güvenlik Önlemleri

Listede görüldüğü gibi 15.000 $'lık bütçe dahilinde azaltılabilecek yalnızca 7 (yedi) risk bulunmaktadır. Seçilen bu önlemler toplu olarak, öncelikle en kritik ve uygun maliyetli riskleri ele alarak şirketin güvenlik duruşunda önemli bir iyileşme sunuyor. Bu önlemler, birim maliyet başına en yüksek risk azaltımını sağladıkları ve belirlenen bütçeye uydukları için seçilmiştir.

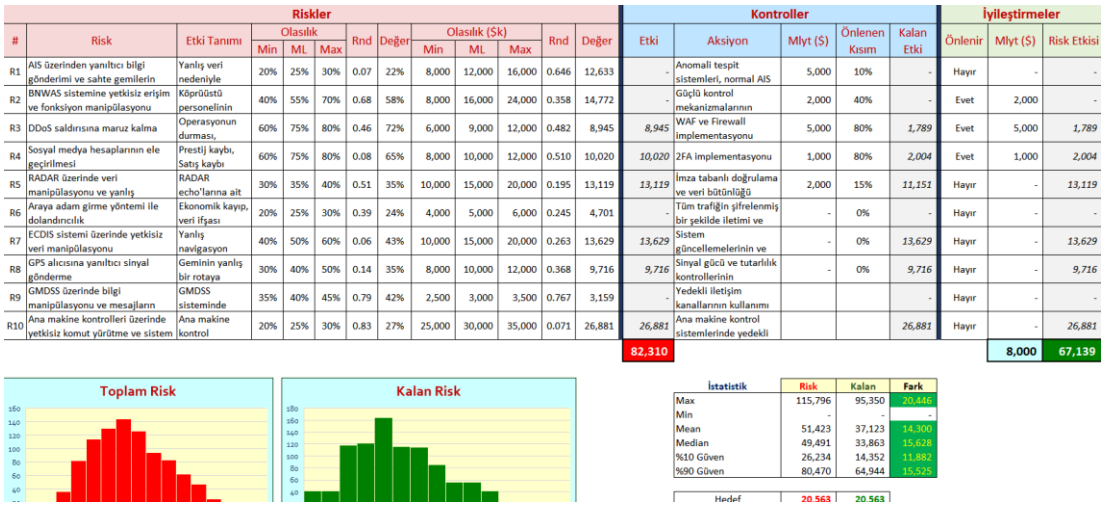


Şekil 4.3: İlk Risk Maliyetleri ve Azaltma Maliyetleri

Listede görüldüğü gibi 15.000 $'lık bütçe dahilinde azaltılabilecek yalnızca 7 (yedi) risk bulunmaktadır. Seçilen bu önlemler toplu olarak, öncelikle en kritik ve uygun maliyetli riskleri ele alarak şirketin güvenlik duruşunda önemli bir iyileşme sunuyor. Bu önlemler, birim maliyet başına en yüksek risk azaltımını sağladıkları ve belirlenen bütçeye uydukları için seçilmiştir.

Çalışmada ayrıca, oluşturmuş olduğumuz çerçevenin tam teşekküllü kullanımı ve tüm bileşenlere ait riskleri ve bunlara karşı alınabilecek önlemler ile oluşacak maliyetlerin ölçümünü tek bir merkezden görmek için tüm formüller Excel üzerinden işlenmiştir. Oluşturulan Excel sayfada istenildiği miktarda Risk ID'si girilebilmektedir.

Her risk için tanım, etki tanımı, Min/ML/Max olasılık değerleri, Min/ML/Max Mali kayıp değerleri, hesaplanan yüzdelikler ve finansal değerler ile kontroller ve iyileştirme sonucu oluşan nihai değerler gösterilmektedir.



	Riskler												Kontroller					İyileştirmeler		
#	Risk	Etki Tanımı	Olasılık			Rnd	Değer	Olasılık ($k)			Rnd	Değer	Etki	Aksiyon	Mlyt ($)	Önlenen Kısım	Kalan Etki	Önlenir	Mlyt ($)	Risk Etkisi
			Min	ML	Max			Min	ML	Max										
R1	AIS üzerinden yanıltıcı bilgi gönderimi ve sahte gemilerin	Yanlış veri nedeniyle	20%	25%	30%	0.07	22%	8,000	12,000	16,000	0.646	12,633	-	Anomali tespit sistemleri, normal AIS	5,000	10%	-	Hayır	-	-
R2	BNWAS sistemine yetkisiz erişim ve fonksiyon manipülasyonu	Köprüüstü personelinin	40%	55%	70%	0.68	58%	8,000	16,000	24,000	0.358	14,772	-	Güçlü kontrol mekanizmalarının	2,000	40%	-	Evet	2,000	-
R3	DDoS saldırısına maruz kalma	Operasyonun durması,	60%	75%	80%	0.46	72%	6,000	9,000	12,000	0.482	8,945	*8,945*	WAF ve Firewall implementasyonu	5,000	80%	*1,789*	Evet	5,000	*1,789*
R4	Sosyal medya hesaplarının ele geçirilmesi	Prestij kaybı, Satış kaybı	60%	75%	80%	0.08	65%	8,000	10,000	12,000	0.510	10,020	*10,020*	2FA implementasyonu	1,000	80%	*2,004*	Evet	1,000	*2,004*
R5	RADAR üzerinde veri manipülasyonu ve yanlış	RADAR echo'larına ait	30%	35%	40%	0.51	35%	10,000	15,000	20,000	0.195	13,119	*13,119*	İmza tabanlı doğrulama ve veri bütünlüğü	2,000	15%	*11,151*	Hayır	-	*13,119*
R6	Araya adam girme yöntemi ile dolandırıcılık	Ekonomik kayıp, veri ifşası	20%	25%	30%	0.39	24%	4,000	5,000	6,000	0.245	4,701	-	Tüm trafiğin şifrelenmiş bir şekilde iletimi ve	-	0%	-	Hayır	-	-
R7	ECDIS sistemi üzerinde yetkisiz veri manipülasyonu	Yanlış navigasyon	40%	50%	60%	0.06	43%	10,000	15,000	20,000	0.263	13,629	*13,629*	Sistem güncellemelerinin ve	-	0%	*13,629*	Hayır	-	*13,629*
R8	GPS alıcısına yanıltıcı sinyal gönderme	Geminin yanlış bir rotaya	30%	40%	50%	0.14	35%	8,000	10,000	12,000	0.368	9,716	*9,716*	Sinyal gücü ve tutarlılık kontrollerinin	-	0%	*9,716*	Hayır	-	*9,716*
R9	GMDSS üzerinde bilgi manipülasyonu ve mesajların	GMDSS sisteminde	35%	40%	45%	0.79	42%	2,500	3,000	3,500	0.767	3,159	-	Yedekli iletişim kanallarının kullanımı			-	Hayır	-	-
R10	Ana makine kontrolleri üzerinde yetkisiz komut yürütme ve sistem	Ana makine kontrol	20%	25%	30%	0.83	27%	25,000	30,000	35,000	0.071	26,881	*26,881*	Ana makine kontrol sistemlerinde yedekli			*26,881*	Hayır	-	*26,881*
													82,310						8,000	67,139

İstatistik	Risk	Kalan	Fark
Max	115,796	95,350	20,446
Min	-	-	-
Mean	51,423	37,123	14,300
Median	49,491	33,863	15,628
%10 Güven	26,234	14,352	11,882
%90 Güven	80,470	64,944	15,525
Hedef	20,563	20,563	

Şekil 4.4: Risk Analizi İçin Oluşturulan Excel Çalışma

Yukarıda yer alan figürde de görüldüğü üzere, öncelikle bir risk envanteri oluşturulmuş, daha sonra MITRE CAPEC ID'ler üzerinden, gemi bileşenleri için risk tanımları ve etki tanımları yapılmıştır. Daha sonra nitel ve nicel risk analiz yöntemlerinin birleşimi olarak ifade edilebilecek bir hibrit olasılık değerlendirmesi yapılmıştır.

Kontroller, riskin önlenen kısmı ve gerekli maliyet gibi verilerin girilmesinin ardından Excel üzerinden, belirlenen tüm riskler Monte Carlo simülasyonundan geçirilerek, 1.000.000 kez senaryo üretilmiş ve sonuçlar sayfaya yazdırılmıştır.

5. TARTIŞMA VE SONUÇ

MITRE CAPEC'i temel alan Monte Carlo simülasyonu temelli bir siber risk çerçevesinin denizcilik endüstrisine entegrasyonu, modern gemilerin ortaya çıkan siber tehditlere karşı korunmasında stratejik bir önem taşımaktadır. Gemi bileşenleri, liman operasyonları ve tedarik zinciri süreçleri gibi birçok kritik unsur, dijitalleşmenin getirdiği karmaşıklıkla birlikte artan siber güvenlik risklerine maruz kalmaktadır.

Bu çerçeve, her bir gemi bileşeniyle ilişkili riskleri kapsamlı bir şekilde değerlendirip azaltmayı hedefleyerek, niteliksel ve niceliksel analizleri bir araya getiren sağlam bir metodoloji sunar. Bu çalışma, Çarpan Etkisi Yaklaşımı ve geleneksel risk yönetimi yöntemlerini kullanarak, kritik deniz varlıklarının güvenliğini ön planda tutan ayrıntılı bir risk hesaplama modeli geliştirmektedir.

Denizcilik sektörü, karmaşık gemi, liman ve tedarik zincirleri ağıyla, dijital teknolojilere olan bağımlılığın artması nedeniyle siber tehditlere karşı özellikle savunmasız bir duruma gelmiştir. Bu bağlamda, çalışma, sistematik risk değerlendirmesi ve proaktif siber güvenlik önlemleri yoluyla bu güvenlik açıklarını anlamanın ve ele almanın kritik önemini vurgulamaktadır.

Geliştirilen risk hesaplama tablosu, siber tehditlerin etkisinin hassas bir şekilde değerlendirilmesine olanak tanıyarak güvenlik çalışmalarının en kritik alanlara odaklanmasını sağlar. Denizcilik işletmeleri, belirli saldırı modellerini ve bunlara karşılık gelen azaltma stratejilerini belirleyerek siber güvenlik duruşlarını ve potansiyel aksaklıklara karşı dayanıklılıklarını geliştirebilirler.

Risk azaltımına ilişkin kararların alınması, denizcilik işletmeleri için büyük bir stratejik öneme sahiptir. Özellikle belirli bir bütçe dahilinde risk azaltımına öncelik vermek, karmaşık bir süreç olabilir. Bu noktada, çerçeve, Optimum Maliyet Dengesi Algoritmasını kullanarak risk etkilerini ve azaltma maliyetlerini hesaplayarak karar vericilere önemli bir destek sunmaktadır. Bu algoritma, sınırlı

kaynakların en verimli şekilde kullanılmasını sağlayarak, işletmelerin en kritik risklerle başa çıkmalarına yardımcı olmaktadır.

Optimum Maliyet Dengesi Algoritması, denizcilik işletmelerine belirli bir bütçe dahilinde risk azaltımına öncelik vermeleri için sistematik ve rasyonel bir yöntem sunmaktadır. Çalışma kapsamında geliştirilen Python tabanlı araç, görsel ve kullanıcı dostu bir arayüzle genişletilebilir. Bu aracın profesyonel bir web tabanlı platforma dahil edilmesi, özellikle denizcilik sektörüne yönelik bir Hizmet Olarak Yazılım (SaaS) çözümü olarak sunulmasını mümkün kılabilir. Böyle bir yaklaşım, yalnızca aracın kullanılabilirliğini ve erişilebilirliğini artırmakla kalmaz, aynı zamanda gerçek zamanlı risk değerlendirmesi ve karar almayı da kolaylaştırır.

Gelecekteki araştırmalar, denizcilik endüstrisine yönelik siber risk çerçevesini daha da geliştirerek sektördeki siber güvenlik sorunlarına yenilikçi çözümler sunabilir. Önemli gelişim alanlarından biri, saldırı modeli veritabanını sürekli güncelleyerek yeni ortaya çıkan tehditleri içerecek şekilde genişletmektir. Bu genişleme, potansiyel tehditler ve uygun azaltma stratejileri hakkında daha kapsamlı bir bakış açısı sağlamaya yardımcı olabilir.

Ayrıca, saldırıların karmaşıklığı arttıkça, gerçek zamanlı tehdit istihbaratı ve makine öğrenimi tabanlı tahmin modellerinin entegrasyonu, risk hesaplamalarının doğruluğunu ve dayanıklılığını önemli ölçüde artırabilir. Çerçevenin daha dinamik ve adaptif hale getirilmesi, özellikle çevresel ve operasyonel değişikliklere hızlı tepki verebilme yeteneği açısından kritik bir öneme sahiptir.

Gerçek zamanlı veri akışlarına dayalı dinamik risk modelleri geliştirmek, denizcilik operasyonlarının siber güvenlik açısından sürekli olarak optimize edilmesine olanak tanır. Bu bağlamda, yapay zeka ve makine öğrenimi tekniklerinin kullanımı, risk senaryolarının daha doğru ve zamanında değerlendirilmesini sağlayabilir. Ayrıca, bu tür modellerin geliştirilmesi sırasında finansal etki değerlendirmelerinin dahil edilmesi, risk yönetimi stratejilerinin maliyet-fayda analizini de güçlendirebilir.

Gelecekteki araştırmalar için bir diğer kritik alan, çerçevenin kapsamlı vaka çalışmaları ve gerçek dünya uygulamaları yoluyla test edilmesi ve doğrulanmasıdır. Birden fazla gemi ve limanda gerçekleştirilecek boylamsal vaka çalışmaları, çerçevenin zaman içindeki etkinliği ve esnekliği hakkında değerli veriler

sağlayabilir. Ayrıca, bu tür çalışmalar, çerçevenin ticari denizcilik, askeri deniz operasyonları, açık deniz platformları ve liman yönetimi gibi çeşitli denizcilik uygulamalarında uyarlanabilirliğini ve etkinliğini test etme fırsatı sunabilir. Farklı bağlamlarda elde edilen sonuçlar, çerçevenin daha geniş bir yelpazede uygulanabilirliğini değerlendirme açısından önemli katkılar sağlayabilir.

Son olarak, politika ve düzenleyici çerçevelerin yanı sıra insan faktörlerine ve eğitime odaklanmak, denizcilik siber güvenliğini iyileştirmede önemli ilerlemeler sağlayabilir. İnsan davranışının siber güvenlik üzerindeki etkisini analiz etmek ve buna dayalı simülasyon tabanlı eğitim programları geliştirmek, gemi personelinin ve diğer paydaşların farkındalığını artırabilir. Aynı zamanda, mevcut denizcilik siber güvenlik politikalarının etkinliğini incelemek, sektördeki düzenleyici boşlukları ve iyileştirme alanlarını ortaya çıkarabilir. Bu tür çalışmalar, denizcilik sektöründe siber güvenlik kültürünün yerleşmesine ve bu alandaki politikaların daha etkin hale getirilmesine katkıda bulunabilir.

Disiplinlerarası araştırmaların teşvik edilmesi ve kamu-özel sektör ortaklıklarının kurulması, denizcilik sektöründe siber güvenlik yenilikçiliğini artırabilir ve sektörel işbirliklerini güçlendirebilir. Bu tür işbirlikleri, siber tehditlerle mücadelede daha bütüncül ve kapsamlı yaklaşımlar geliştirilmesine olanak tanımaktadır. Gelecekteki çalışmalar, bu araştırma yönlerini keşfederek denizcilik siber güvenliğinin geliştirilmesine katkıda bulunabilir ve sektörün hızla gelişen tehditlerle başa çıkmaya daha hazırlıklı olmasını sağlayabilir. Bu alandaki ilerlemeler, denizcilik endüstrisinin rekabet gücünü ve sürdürülebilirliğini artırarak, küresel tedarik zincirlerinin güvenliğini sağlamaya da katkı sunacaktır.

KAYNAKLAR

Abdullayev, V. and Chauhan, A. S. (2023). Sql injection attack: quick view. Mesopotamian Journal of Cyber Security, 30-34. https://doi.org/10.58496/mjcs/2023/006

Adu, K. O. and Adjei, E. (2018). The phenomenon of data loss and cyber security issues in ghana. Foresight, 20(2), 150-161. https://doi.org/10.1108/fs-08-2017-0043

Ahangama, S. (2023). Relating social media diffusion, education level and cybersecurity protection mechanisms to e-participation initiatives: insights from a cross-country analysis. Information Systems Frontiers, 25(5), 1695-1711. https://doi.org/10.1007/s10796-023-10385-7

Ahmadi, V., Arlos, P., & Casalicchio, E. (2021). Normalization framework for vulnerability risk management in cloud. 2021 8th International Conference on Future Internet of Things and Cloud (FiCloud). https://doi.org/10.1109/ficloud49777.2021.00022

Alashi, S. A. and Badi, D. H. (2020). The role of governance in achieving sustainable cybersecurity for business corporations. Journal of Information Security and Cybercrimes Research, 3(1), 97-112. https://doi.org/10.26735/eint7997

Alcántara, M. and Melgar, A. (2016). Risk management in information security: a systematic review. Journal of Advances in Information Technology, 7(1), 1-7. https://doi.org/10.12720/jait.7.1.1-7

Alekseievska, H. and Ilchenko, S. (2023). Methodological foundations for assessing the efficiency of maritime transport enterprises in meeting the needs of the national economy. Three Seas Economic Journal, 4(4), 1-10. https://doi.org/10.30525/2661-5150/2023-4-1

Algarni, A. and Thayananthan, V. (2023). Autonomous vehicles with a 6g-based intelligent cybersecurity model. IEEE Access, 11, 15284-15296. https://doi.org/10.1109/access.2023.3244883

AL-Hawamleh, A. M. (2023). Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures. International Journal of Advanced Computer Science and Applications, 14(2). https://doi.org/10.14569/ijacsa.2023.0140292

Ali, N. A. R. A., Chebotareva, A. A., & Chebotarev, V. E. (2021). Cyber security in marine transport. Pomorstvo, 35(2), 248-255. https://doi.org/10.31217/p.35.2.7

Alzamil, Z. A. (2018). Information security practice in saudi arabia: case study on saudi organizations. Information &Amp; Computer Security, 26(5), 568-583. https://doi.org/10.1108/ics-01-2018-0006

Alzayedi, A. M. T., Batra, A., Sampath, S., & Pilidis, P. (2022). Techno-environmental mission evaluation of combined cycle gas turbines for large container ship propulsion. Energies, 15(12), 4426. https://doi.org/10.3390/en15124426

Amah, U., Mart, J., & Oyetoro, A. (2023). Cloud security governance guidelines.. https://doi.org/10.14293/pr2199.000062.v1

Amini, A., Jamil, N., Ahmad, A. R., & Z'aba, M. R. (2015). Threat modeling approaches for securing cloud computin. Journal of Applied Sciences, 15(7), 953-967. https://doi.org/10.3923/jas.2015.953.967

Antonopoulos, M., Drainakis, G., Ouzounoglou, E., Papavassiliou, G., & Amditis, A. (2022). Design and proof of concept of a prediction engine for decision support during cyber range attack simulations in the maritime domain. 2022 IEEE International Conference on Cyber Security and Resilience (CSR). https://doi.org/10.1109/csr54599.2022.9850280

Antunes, M., Silva, C., & Marques, F. (2021). An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context. Applied Sciences, 11(23), 11269. https://doi.org/10.3390/app112311269

Anwar, M., He, W., Ash, I. K., Yuan, X., Li, L., & Xu, L. D. (2017). Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 69, 437-443. https://doi.org/10.1016/j.chb.2016.12.040

Aşan, C. (2023). Mersin University Journal of Maritime Faculty. The Role of Cyber Situational Awareness of Humans in Social Engineering Cyber Attacks on the Maritime Domain.

Aslan, Ö. and Samet, R. (2020). A comprehensive review on malware detection approaches. IEEE Access, 8, 6249-6271. https://doi.org/10.1109/access.2019.2963724

Aspers, P. and Corte, U. (2021). What is qualitative in research. Qualitative Sociology, 44(4), 599-608. https://doi.org/10.1007/s11133-021-09497-w

Asquith, P. M. and Morgan, P. L. (2020). Representing a human-centric cyberspace. Advances in Intelligent Systems and Computing, 122-128. https://doi.org/10.1007/978-3-030-52581-1_16

Atakisi, A. and Cebeci, A. (2022). Kalkınma planlarının kıyaslamalı analizi: türkiye örneği. Ekonomi Ve Finansal Araştırmalar Dergisi, 4(2), 157-172. https://doi.org/10.56668/jefr.1123716

August, T., Dao, D., & Niculescu, M. (2022). Economics of ransomware: risk interdependence and large-scale attacks. Management Science, 68(12), 8979-9002. https://doi.org/10.1287/mnsc.2022.4300

Australian National Audit Office. (2014). Cyber Attacks: Securing Agencies' ICT Systems. Erişim adresi: https://www.anao.gov.au/work/performance-audit/cyber-attacks-securing-agencies-ict-systems

Aydın, M., Bütün, İ., Biçakcı, K., & Baykal, N. (2020). Using attribute-based feature selection approaches and machine learning algorithms for detecting fraudulent website urls. 2020 10th Annual Computing and

Communication Workshop and Conference (CCWC). https://doi.org/10.1109/ccwc47524.2020.9031125

Back, S. and Guerette, R. T. (2021). Cyber place management and crime prevention: the effectiveness of cybersecurity awareness training against phishing attacks. Journal of Contemporary Criminal Justice, 37(3), 427-451. https://doi.org/10.1177/10439862211001628

Bailetti, T. and Craigen, D. (2020). Examining the relationship between cybersecurity and scaling value for new companies. Technology Innovation Management Review, 10(2), 62-69. https://doi.org/10.22215/timreview/1329

Balthrop, J., Forrest, S., Newman, M. E. J., & Williamson, M. M. (2004). Technological networks and the spread of computer viruses. Science, 304(5670), 527-529. https://doi.org/10.1126/science.1095845

Bank Info Security. (2018). Ransomware Crypto-Locks Port of San Diego IT Systems. Erişim adresi: https://www.bankinfosecurity.com/ransomware-crypto-locks-port-san-diego-systems-a-11571

Baran, S. and Şener, E. (2019). Hastanelerde bilgi güvenliği yönetimi: nitel bir araştirma. Süleyman Demirel Üniversitesi Vizyoner Dergisi, 10(23), 108-125. https://doi.org/10.21076/vizyoner.444451

Barić, M., Čulin, J., & Bielić, T. (2018). Problems that occur in a team: learning from maritime accidents via simulation training. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, 12(4), 709-713. https://doi.org/10.12716/1001.12.04.09

Batalden, B. and Sydnes, A. K. (2013). Maritime safety and the ism code: a study of investigated casualties and incidents. WMU Journal of Maritime Affairs, 13(1), 3-25. https://doi.org/10.1007/s13437-013-0051-8

BBC. (2016). North Korea 'jamming GPS signals' near South border. Erişim adresi: https://www.bbc.com/news/world-asia-35940542

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: recent advances, analysis, challenges and future research directions. Computers &Amp; Security, 111, 102490. https://doi.org/10.1016/j.cose.2021.102490

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K. M., & Meskin, N. (2020). Cybersecurity for industrial control systems: a survey. Computers &Amp; Security, 89, 101677. https://doi.org/10.1016/j.cose.2019.101677

Biçakcı, K., Ünal, D., Ascioglu, N., & Adalier, O. (2014). Mobile authentication secure against man-in-the-middle attacks. 2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering. https://doi.org/10.1109/mobilecloud.2014.43

Boston Magazine. (2014). Mass. Maritime Website Hacked by Islamic Extremist Group. Erişim adresi: https://www.bostonmagazine.com/news/2014/10/07/mass-maritime-website-hacked-islamic-extremist-group/

Buil-Gil, D., Lord, N., & Barrett, E. (2021). The dynamics of business, cybersecurity and cyber-victimization: foregrounding the internal

guardian in prevention. Victims &Amp;amp; Offenders, 16(3), 286-315. https://doi.org/10.1080/15564886.2020.1814468

Campbell, R., Gregory, K., Patterson, D., & Bybee, D. (2012). Integrating qualitative and quantitative approaches: an example of mixed methods research.. Methodological Approaches to Community-Based Research., 51-68. https://doi.org/10.1037/13492-004

Chen, Z., Guo, M., & Zhou, L. (2018). Research on sql injection detection technology based on svm. MATEC Web of Conferences, 173, 01004. https://doi.org/10.1051/matecconf/201817301004

Chu, W., Lin, C., & Chang, K. (2019). Detection and classification of advanced persistent threats and attacks using the support vector machine. Applied Sciences, 9(21), 4579. https://doi.org/10.3390/app9214579

Conti, M., Gangwal, A., & Ruj, S. (2018). On the economic significance of ransomware campaigns: a bitcoin transactions perspective. Computers &Amp;amp; Security, 79, 162-189. https://doi.org/10.1016/j.cose.2018.08.008

Crihan, G., Craciun, M., & Dumitriu, L. (2023). Hybrid methods of authentication in network security. The Annals of "Dunarea De Jos" University of Galati. Fascicle III, Electrotechnics, Electronics, Automatic Control, Informatic, 45(1), 7. https://doi.org/10.35219/eeaci.2022.1.02

Cruise Law News. (2020). AIDA Cruise Ships Under Cyber Attack – Are Costa Ships Also Affected?. Erişim adresi: https://www.cruiselawnews.com/2020/12/articles/cyber-attacks/aida-cruise-ships-under-cyber-attack-are-costa-ships-also-affected/

Cruise Mapper. (2021). Carnival Corporation customers were affected by data breach on March 19. Erişim adresi: https://www.cruisemapper.com/news/9025-carnival-corp.-customers-were-affected-by-data-breach-on-march-19

Dambra, S., Bilge, L., & Balzarotti, D. (2023). A comparison of systemic and systematic risks of malware encounters in consumer and enterprise environments. ACM Transactions on Privacy and Security, 26(2), 1-30. https://doi.org/10.1145/3565362

Data Breach Today. (2014). Navy Systems Admin. Faces Hacking Charge. Erişim adresi: https://www.databreachtoday.asia/navy-systems-admin-faces-hacking-charge-a-6816

Demirci, S. M. E. and Çiçek, K. (2022). Innovative strategy development approach for enhancing the effective implementation of the international safety management (ism) code. Transportation Research Record: Journal of the Transportation Research Board, 2677(1), 25-48. https://doi.org/10.1177/03611981221098394

Demirel, T. and Işcan, İ. H. (2021). Diş ticaretin ekonomik büyüme üzerine etkisi: güney kore ve türkiye örneğiyle bir eşbütünleşme analizi. International Journal of Management Economics and Business, 17(1), 1-27. https://doi.org/10.17130/ijmeb.794267

Dimakopoulou, A. and Rantos, K. (2024). Comprehensive analysis of maritime cybersecurity landscape based on the nist csf v2.0. Journal of Marine

Science and Engineering, 12(6), 919. https://doi.org/10.3390/jmse12060919

Dimitriadis, A., Lontzetidis, E., Kulvatunyou, B., Ivezic, N., Gritzalis, D., & Mavridis, I. (2023). Fronesis: digital forensics-based early detection of ongoing cyber-attacks. IEEE Access, 11, 728-743. https://doi.org/10.1109/access.2022.3233404

Dinev, T. and Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. Journal of the Association for Information Systems, 8(7), 386-408. https://doi.org/10.17705/1jais.00133

Dorta-González, P., Peñate, D. R. S., & Suárez-Vega, R. (2002). Untitled. Annals of Operations Research, 116(1/4), 129-152. https://doi.org/10.1023/a:1021380314032

Dou, Y., Wang, C., Gu, C., O'Neill, M., & Liu, W. (2021). Design and analysis of hardware trojans in approximate circuits. Electronics Letters, 58(5), 197-199. https://doi.org/10.1049/ell2.12405

Drlling Contractor. (2015). Industry recognizing need for better cyber defenses as hackers become more sophisticated and drilling equipment becomes more interconnected. Erişim adresi: https://drillingcontractor.org/drilling-cybersecurity-36727

Dvořák, Z., Řehák, D., Dávid, A., & Čekerevac, Z. (2020). Qualitative approach to environmental risk assessment in transport. International Journal of Environmental Research and Public Health, 17(15), 5494. https://doi.org/10.3390/ijerph17155494

Erick, O., Andrew, M., & Agnes, N. (2019). Information security policy compliance: a broad-based literature review and a theoretical framework. International Journal of Computer Applications, 181(47), 8-13. https://doi.org/10.5120/ijca2019918519

Fahmi Rifai, Jazman, M., Angraini, A., & Megawati, M. (2023). Design of application information security self-assessment using vba and msxml2.xmlhttp case study: diskominfo kabupaten kampar. Jurnal Teknik Informatika (Jutif), 4(6), 1523-1534. https://doi.org/10.52436/1.jutif.2023.4.6.1033

Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V. L., Gordon, L. A., … & Lin, H. (2019). Cyber risk research impeded by disciplinary barriers. Science, 366(6469), 1066-1069. https://doi.org/10.1126/science.aaz4795

Fathurohman, A. and Witjaksono, R. W. (2020). Analysis and design of information security management system based on iso 27001: 2013 using annex control (case study: district of government of bandung city). Bulletin of Computer Science and Electrical Engineering, 1(1), 1-11. https://doi.org/10.25008/bcsee.v1i1.2

Freire, W. P., Melo, W. S., Nascimento, V. D. d., Nascimento, P. R., & Sá, A. O. d. (2022). Towards a secure and scalable maritime monitoring system using blockchain and low-cost iot technology. Sensors, 22(13), 4895. https://doi.org/10.3390/s22134895

Frisk, I., Ruoslahti, H., & Tikanmäki, I. (2023). Cybersecurity through thesis in laurea university of applied sciences. European Conference on Cyber Warfare and Security, 22(1), 484-492. https://doi.org/10.34190/eccws.22.1.1447

gCaptain. (2018). Clarkson Plc Reveals Details of 2017 Cyber Security Incident. Erişim adresi: https://gcaptain.com/clarkson-plc-reveals-details-of-2017-cyber-security-incident/

gCaptain. (2022). Cyber Pirates Prowling Ship Controls Threaten Another Big Supply Chain Shock. Erişim adresi: https://gcaptain.com/cyber-pirates-prowling-ship-controls-threaten-another-big-supply-chain-shock/

Gcaza, N. and Solms, R. v. (2017). Cybersecurity culture: an ill-defined problem. IFIP Advances in Information and Communication Technology, 98-109. https://doi.org/10.1007/978-3-319-58553-6_9

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. Sensors, 21(9), 3267. https://doi.org/10.3390/s21093267

Giudici, P. and Raffinetti, E. (2021). Explainable ai methods in cyber risk management. Quality and Reliability Engineering International, 38(3), 1318-1326. https://doi.org/10.1002/qre.2939

Graham, C. A. E. and Walters, D. (2020). Representation of seafarers' occupational safety and health: limits of the maritime labour convention. The Economic and Labour Relations Review, 32(2), 266-282. https://doi.org/10.1177/1035304620981374

Graham, S. (2004). The end of geography or the explosion of place? conceptualizing space, place, and information technology. Reading Economic Geography, 336-349. https://doi.org/10.1002/9780470755716.ch21

Guetterman, T. C., Fetters, M. D., & Creswell, J. W. (2015). Integrating quantitative and qualitative results in health science mixed methods research through joint displays. The Annals of Family Medicine, 13(6), 554-561. https://doi.org/10.1370/afm.1865

Güler, C. ve Furat, F. (2022). Belge yönetimi ve arşiv uygulamalarının bilgi güvenliği ilkelerine katkısı: kavramsal bir değerlendirme. Turk Kutuphaneciligi - Turkish Librarianship, 36(1), 6-6. https://doi.org/10.24146/tk.1012325

Gündüzalp, C. (2021). University employees' awareness of digital data and personal cyber security (a case study of it departments). Journal of Computer and Education Research, 9(18), 598-625. https://doi.org/10.18009/jcer.907022

Güven, A. F. and Yörükeren, N. (2022). Energy management and optimization of a hybrid energy system by particle swarm optimizing algorithm-genetic algorithm and gray wolf optimizing algorithm technique: a case study for yalova university. Karadeniz Fen Bilimleri Dergisi, 12(2), 853-879. https://doi.org/10.31466/kfbd.1169643

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hadlington, L. (2018). The "human factor" in cybersecurity. Advances in Digital Crime, Forensics, and Cyber Terrorism, 46-63. https://doi.org/10.4018/978-1-5225-4053-3.ch003

Han, L., Zhou, M., Han, S., Jia, W., Sun, C., & Fu, C. (2018). Targeting malware discrimination based on reversed association task. Concurrency and Computation: Practice and Experience, 31(23). https://doi.org/10.1002/cpe.4922

Haner, M., Sloan, M. M., Graham, A., Pickett, J. T., & Cullen, F. T. (2022). Ransomware and the robin hood effect?: experimental evidence on americans' willingness to support cyber-extortion. Journal of Experimental Criminology. https://doi.org/10.1007/s11292-022-09515-z

Hariharan, M., K, A. H., & Prasad, B. G. (2019). Ddos attack detection using c5.0 machine learning algorithm. International Journal of Wireless and Microwave Technologies, 9(1), 52-59. https://doi.org/10.5815/ijwmt.2019.01.06

Hasanov, N. and Alsulaiman, M. F. (2021). Evaluating the implementation framework of the international ship and port facility security code in the republic of azerbaijan. Maritime Technology and Research, 3(2), 185-201. https://doi.org/10.33175/mtr.2021.247419

Helms, M. M. and Nixon, J. (2010). Exploring swot analysis – where are we now?. Journal of Strategy and Management, 3(3), 215-251. https://doi.org/10.1108/17554251011064837

Hou, X., Wang, J., Bai, T., Deng, Y., Ren, Y., & Hanzo, L. (2023). Environment-aware auv trajectory design and resource management for multi-tier underwater computing. IEEE Journal on Selected Areas in Communications, 41(2), 474-490. https://doi.org/10.1109/jsac.2022.3227103

Howah, K. and Chugh, R. (2019). Do we trust the internet?. Journal of Global Information Management, 27(3), 87-100. https://doi.org/10.4018/jgim.2019070105

Ibrahim, A. M. (2024). The influence of computerized simulation techniques on maritime security exercises: isps code. Maritime Research and Technology, 3(1), 1. https://doi.org/10.21622/mrt.2024.03.1.747

International Pipeline Resilience Organization. (2021). Port of Houston Cyber-Attack--A Reminder of Risks Close to Home. Erişim adresi: https://www.pipelineresilience.org/news/port-of-houston-cyber-attack-a-reminder-of-risks-close-to-home

Jampen, D., Gür, G., Sutter, T. S., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. a comparative literature review. Human-Centric Computing and Information Sciences, 10(1). https://doi.org/10.1186/s13673-020-00237-7

Javeed, D., MohammedBadamasi, U., Ndubuisi, C., Soomro, N. F., & Asif, M. (2020). Man in the middle attacks: analysis, motivation and prevention. International Journal of Computer Networks and Communications Security, 8(7), 52-58. https://doi.org/10.47277/ijcncs/8(7)1

Jevelin, J. and Faza, A. (2023). Evaluation the information security management system: a path towards iso 27001 certification. Journal of Information Systems and Informatics, 5(4), 1240-1256. https://doi.org/10.51519/journalisi.v5i4.572

Joseph, A. and Dalaklis, D. (2021). The international convention for the safety of life at sea: highlighting interrelations of measures towards effective risk mitigation. Journal of International Maritime Safety, Environmental Affairs, and Shipping, 5(1), 1-11. https://doi.org/10.1080/25725084.2021.1880766

Joubert, F. and Pretorius, L. (2017). Using monte carlo simulation to create a ranked check list of risks in a portfolio of railway construction projects. South African Journal of Industrial Engineering, 28(2). https://doi.org/10.7166/28-2-1604

Jupp, V. (2006). The Sage dictionary of social research methods. The SAGE Dictionary of Social Research Methods, 1-352

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring sme cybersecurity practices in developing countries. Journal of Organizational Computing and Electronic Commerce, 28(3), 269-282. https://doi.org/10.1080/10919392.2018.1484598

Kanaker, H., Karim, N. A., Awwad, S. A. B., Ismail, N. H. A., Zraqou, J., & ali, A. M. F. A. (2022). Trojan horse infection detection in cloud based environment using machine learning. International Journal of Interactive Mobile Technologies (iJIM), 16(24), 81-106. https://doi.org/10.3991/ijim.v16i24.35763

Kang, S. (2007). Disembodiment in online social interaction: impact of online chat on social support and psychosocial well-being. CyberPsychology &Amp; Behavior, 10(3), 475-477. https://doi.org/10.1089/cpb.2006.9929

Kanığ, M. (2020). Investigation of the relationship between perceived social support level and healthy lifestyle behaviors. Journal of Psychiatric Nursing. https://doi.org/10.14744/phd.2020.89156

Kanwal, K., Shi, W., Kontovas, C. A., Yang, Z., & Chang, C. (2022). Maritime cybersecurity: are onboard systems ready?. Maritime Policy &Amp; Management, 51(3), 484-502. https://doi.org/10.1080/03088839.2022.2124464

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., & Davidson, I. E. (2021). Ransomware detection, avoidance, and mitigation scheme: a review and future directions. Sustainability, 14(1), 8. https://doi.org/10.3390/su14010008

Kayisoglu, G., Bolat, P., & Tam, K. (2022). Evaluating slim-based human error probability for ecdis cybersecurity in maritime. Journal of Navigation, 75(6), 1364-1388. https://doi.org/10.1017/s0373463322000534

Keçeci, T. (2021). Fuzzy multiple-criteria decision making based evaluation of the incident analysis forms used in internal reporting systems: a case study of tanker shipping companies. Transportation Research Record: Journal of the Transportation Research Board, 2676(3), 758-771. https://doi.org/10.1177/03611981211056915

Keleştemur, A. (2015). Siber İstihbarat, Level Kitap.

Kimpe, L. D., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, i need somebody: examining the antecedents of social support seeking among cybercrime victims. Computers in Human Behavior, 108, 106310. https://doi.org/10.1016/j.chb.2020.106310

King, Z. M., Henshel, D. S., Flora, L., Cains, M., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. Frontiers in Psychology, 9. https://doi.org/10.3389/fpsyg.2018.00039

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2022). Developing a risk analysis strategy framework for impact assessment in information security management systems: a case study in it consulting industry. Sustainability, 14(3), 1269. https://doi.org/10.3390/su14031269

Koç, K. and Güven, Ş. D. (2023). Nevşehir devlet hastanesinde çalişan hekim ve hemşirelerin kalite algilarinin belirlenmesi. Nevşehir Hacı Bektaş Veli Üniversitesi SBE Dergisi, 13(2), 827-842. https://doi.org/10.30783/nevsosbilen.1135176

Köhler, T., Smith, A. D., & Bhakoo, V. (2018). Feature topic for orm: "templates in qualitative research methods". Organizational Research Methods, 22(1), 3-5. https://doi.org/10.1177/1094428118805165

Kolcu, M. and Bülbül, E. (2023). Covid-19 korkusunun aşılanmaya ve ölüm anksiyetesine etkisi. Turkish Journal of Family Medicine and Primary Care, 17(4), 489-496. https://doi.org/10.21763/tjfmpc.1242149

Kolosnjaji, B., Demontis, A., Biggio, B., Maiorca, D., Giacinto, G., Eckert, C., … & Roli, F. (2018). Adversarial malware binaries: evading deep learning for malware detection in executables. 2018 26th European Signal Processing Conference (EUSIPCO). https://doi.org/10.23919/eusipco.2018.8553214

Kothawade, S. (2022). Malware: concepts and principles.. https://doi.org/10.31219/osf.io/fg954

Kuerbis, B. and Badiei, F. (2017). Mapping the cybersecurity institutional landscape. Digital Policy, Regulation and Governance, 19(6), 466-492. https://doi.org/10.1108/dprg-05-2017-0024

Kuhn, K., Bicakci, S., & Shaikh, S. A. (2021). Covid-19 digitization in maritime: understanding cyber risks. WMU Journal of Maritime Affairs, 20(2), 193-214. https://doi.org/10.1007/s13437-021-00235-1

Kumar, S. and Singh, M. (2017). Detection and isolation of zombie attack under cloud environment. Oriental Journal of Computer Science and Technology, 10(2), 338-344. https://doi.org/10.13005/ojcst/10.02.12

Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Computing and Applications, 34(18), 15241-15271. https://doi.org/10.1007/s00521-022-06959-2

Lam, C. S., Velthoven, M. H. v., & Meinert, E. (2020). Application of internet of things in cell-based therapy delivery: protocol for a systematic review. JMIR Research Protocols, 9(3), e16935. https://doi.org/10.2196/16935

Li, L., Li, D., Bissyandé, T. F., Klein, J., Traon, Y. L., Lo, D., … & Cavallaro, L. (2017). Understanding android app piggybacking: a systematic study of malicious code grafting. IEEE Transactions on Information Forensics and Security, 12(6), 1269-1284. https://doi.org/10.1109/tifs.2017.2656460

Li, X. and Xue, Y. (2014). A survey on server-side approaches to securing web applications. ACM Computing Surveys, 46(4), 1-29. https://doi.org/10.1145/2541315

Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. Entrepreneurship and Sustainability Issues, 4(4), 559-573. https://doi.org/10.9770/jesi.2017.4.4(12)

Liu, W. and Zhong, S. (2017). Web malware spread modelling and optimal control strategies. Scientific Reports, 7(1). https://doi.org/10.1038/srep42308

Liu, Y., Fang, B., Ye, G., Sun, Z., & Tian, Z. (2020). Hierarchically defining internet of things security: from cia to caca. International Journal of Distributed Sensor Networks, 16(1), 155014771989937. https://doi.org/10.1177/1550147719899374

Lopes, I. and Oliveira, P. (2016). Adoption of an information systems security policy in small and medium sized enterprises. Journal of Information Systems Engineering &Amp; Management, 1(1). https://doi.org/10.20897/lectito.201605

Los Angeles Times. (2017). Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks. Erişim adresi: https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html

Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, 13(12), 155014771774146. https://doi.org/10.1177/1550147717741463

Mallik, A., Ahsan, A., Shahadat, M. M. Z., & Tsou, J. (2019). Man-in-the-middle-attack: understanding in simple words. International Journal of Data and Network Science, 77-92. https://doi.org/10.5267/j.ijdns.2019.1.001

Mantoju, C. D. (2021). Analysis of impact of the maritime labour convention, 2006: a seafarer's perspective. Journal of International Maritime Safety, Environmental Affairs, and Shipping, 5(3), 107-119. https://doi.org/10.1080/25725084.2021.1955475

Marinho, R. ve Filho, R. H. (2023). Automated emerging cyber threat identification and profiling based on natural language processing. IEEE Access, 11, 58915-58936. https://doi.org/10.1109/access.2023.3260020

Maritime Executive. (2021). South Korean Shipbuilder DSME Confirms New Possible Cyber Attack. Erişim adresi: https://maritime-executive.com/article/south-korean-shipbuilder-dsme-confirms-new-possible-cyber-attack

Massacci, F. and Tizio, G. D. (2022). Are software updates useless against advanced persistent threats?. Communications of the ACM, 66(1), 31-33. https://doi.org/10.1145/3571452

Mataracioglu, T. and Özkan, S. (2011). Governing information security in conjunction with cobit and iso 27001. International Journal of Network Security &Amp; Its Applications, 3(4), 111-116. https://doi.org/10.5121/ijnsa.2011.3410

Matheu, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2020). A survey of cybersecurity certification for the internet of things. ACM Computing Surveys, 53(6), 1-36. https://doi.org/10.1145/3410160

Matheu, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2020). A survey of cybersecurity certification for the internet of things. ACM Computing Surveys, 53(6), 1-36. https://doi.org/10.1145/3410160

Mavroeidis, V. ve Bromander, S. (2017). Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. 2017 European Intelligence and Security Informatics Conference (EISIC). https://doi.org/10.1109/eisic.2017.20

MCAD Maritime Cyber Attack Database. (2019). Oil Tanker hit by ransomware attack near the Port of Naantali, Finland. Erişim adresi: https://www.maritimecybersecurity.nl/incident/j7NoOqjm5a

McDonald, G., Papadopoulos, P., Pitropakis, N., Ahmad, J., & Buchanan, W. J. (2022). Ransomware: analysing the impact on windows active directory domain services. Sensors, 22(3), 953. https://doi.org/10.3390/s22030953

McGillivary, P. A. (2018). Why maritime cybersecurity is an ocean policy priority and how it can be addressed. Marine Technology Society Journal, 52(5), 44-57. https://doi.org/10.4031/mtsj.52.5.11

McGillivary, P. A. (2018). Why maritime cybersecurity is an ocean policy priority and how it can be addressed. Marine Technology Society Journal, 52(5), 44-57. https://doi.org/10.4031/mtsj.52.5.11

Miraja, B. A., Persada, S. F., Prasetyo, Y. T., Belgiawan, P. F., & Redi, A. A. N. P. (2019). Applying protection motivation theory to understand generation z students intention to comply with educational software anti piracy law. International Journal of Emerging Technologies in Learning (iJET), 14(18), 39. https://doi.org/10.3991/ijet.v14i18.10973

Mirtsch, M., Kinne, J., & Blind, K. (2021). Exploring the adoption of the international information security management system standard iso/iec 27001: a web mining-based analysis. IEEE Transactions on Engineering Management, 68(1), 87-100. https://doi.org/10.1109/tem.2020.2977815

Mohamed, H. A. R. (2014). A proposed model for it disaster recovery plan. International Journal of Modern Education and Computer Science, 6(4), 57-67. https://doi.org/10.5815/ijmecs.2014.04.08

Mylonas, A. and Gritzalis, D. (2012). Practical malware analysis: the hands-on guide to dissecting malicious software. Computers &Amp; Security, 31(6), 802-803. https://doi.org/10.1016/j.cose.2012.05.004

Nafees, M., Saxena, N., Cárdenas, Á. A., Grijalva, S., & Burnap, P. (2023). Smart grid cyber-physical situational awareness of complex operational technology attacks: a review. ACM Computing Surveys, 55(10), 1-36. https://doi.org/10.1145/3565570

Nair, M. G. (2016). A survey of commonly used cryptographic algorithms in information security. International Journal of Engineering and Computer Science. https://doi.org/10.18535/ijecs/v4i11.37

Nawaz, U., Aleem, M., & Lin, J. C. (2022). On the evaluation of android malware detectors against code-obfuscation techniques. PeerJ Computer Science, 8, e1002. https://doi.org/10.7717/peerj-cs.1002

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., … & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: a systematic review. Sensors, 21(15), 5119. https://doi.org/10.3390/s21155119

Nižetić, S., Šolić, P., López-de-Ipiña, D., & Patrono, L. (2020). Internet of things (iot): opportunities, issues and challenges towards a smart and sustainable future. Journal of Cleaner Production, 274, 122877. https://doi.org/10.1016/j.jclepro.2020.122877

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: a human factors problem. HOLISTICA – Journal of Business and Public Administration, 13(1), 49-72. https://doi.org/10.2478/hjbpa-2022-0003

Nobles, C., Burrell, D. N., & Waller, T. (2022). The need for a global aviation cybersecurity defense policy. Land Forces Academy Review, 27(1), 19-26. https://doi.org/10.2478/raft-2022-0003

Offshore Energy. (2020). Hurtigruten comes under cyberattack. Erişim adresi: https://www.offshore-energy.biz/hurtigruten-comes-under-cyberattack/

Orlando, A. (2021). Cyber risk quantification: investigating the role of cyber value at risk. Risks, 9(10), 184. https://doi.org/10.3390/risks9100184

Ozcan, H., Okten, N. Z., & Uzpeder, İ. (2021). Sigorta sektörünün yarattiği kamusal dişsalliklar. Doğuş Üniversitesi Dergisi, 22(2), 73-88. https://doi.org/10.31671/doujournal.972985

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the bitcoin ecosystem. Journal of Cybersecurity, 5(1). https://doi.org/10.1093/cybsec/tyz003

Park, J. S., Seo, Y., & Ha, M. (2019). The role of maritime, land, and air transportation in economic growth: panel evidence from oecd and non-oecd countries. Research in Transportation Economics, 78, 100765. https://doi.org/10.1016/j.retrec.2019.100765

Pelletier, D. ve Wei, W. (2015). The geometric-var backtesting method. Journal of Financial Econometrics, 14(4), 725-745. https://doi.org/10.1093/jjfinec/nbv015

Peng, S., Yu, S., & Yang, A. (2014). Smartphone malware and its propagation modeling: a survey. IEEE Communications Surveys &Amp; Tutorials, 16(2), 925-941. https://doi.org/10.1109/surv.2013.070813.00214

Port Technology International. (2022). Dated security patches potential cause behind European port cyber attacks. Erişim adresi: https://www.porttechnology.org/news/dated-security-patches-potential-cause-behind-european-port-cyber-attacks/

Ports Europe. (2018). Barcelona port suffers cyber attack. Erişim adresi: https://www.portseurope.com/barcelona-port-suffers-a-cyber-attack/

Probst, C. W., Hunker, J., Gollmann, D., & Bishop, M. (2010). Insider threats in cyber security. Advances in Information Security. https://doi.org/10.1007/978-1-4419-7133-3

Qazi, A. and Akhtar, P. (2020). Risk matrix driven supply chain risk management: adapting risk matrix based tools to modelling interdependent risks and risk appetite. Computers &Amp; Industrial Engineering, 139, 105351. https://doi.org/10.1016/j.cie.2018.08.002

Qbea'h, M., Alshraideh, M., & Sabri, K. E. (2016). Detecting and preventing sql injection attacks: a formal approach. 2016 Cybersecurity and Cyberforensics Conference (CCC). https://doi.org/10.1109/ccc.2016.26

Qian, L. (2022). Joint multi-domain resource allocation and trajectory optimization in uav-assisted m-iot networks.. https://doi.org/10.36227/techrxiv.17704463

Quigley, K., Burns, C., & Stallard, K. (2015). 'cyber gurus': a rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. Government Information Quarterly, 32(2), 108-117. https://doi.org/10.1016/j.giq.2015.02.001

Radanliev, P., Roure, D. D., Burnap, P., & Santos, O. (2021). Epistemological equation for analysing uncontrollable states in complex systems: quantifying cyber risks from the internet of things. The Review of Socionetwork Strategies, 15(2), 381-411. https://doi.org/10.1007/s12626-021-00086-5

Raimundo, R. and Rosário, A. T. (2022). Cybersecurity in the internet of things in industrial management. Applied Sciences, 12(3), 1598. https://doi.org/10.3390/app12031598

Rajamäki, J. and Järvinen, M. (2022). Exploring care robots' cybersecurity threats from care robotics specialists' point of view. European Conference on Cyber Warfare and Security, 21(1), 231-238. https://doi.org/10.34190/eccws.21.1.275

Ramachandran, M. and Chang, V. (2014). Recommendations and best practices for cloud enterprise security. 2014 IEEE 6th International Conference on

Cloud Computing Technology and Science. https://doi.org/10.1109/cloudcom.2014.105

Ramlo, S. and Nicholas, J. B. (2021). The human factor: assessing individuals' perceptions related to cybersecurity. Information &Amp; Computer Security, 29(2), 350-364. https://doi.org/10.1108/ics-04-2020-0052

Ramlo, S. and Nicholas, J. B. (2021). The human factor: assessing individuals' perceptions related to cybersecurity. Information &Amp; Computer Security, 29(2), 350-364. https://doi.org/10.1108/ics-04-2020-0052

Ramlo, S. and Nicholas, J. B. (2021). The human factor: assessing individuals' perceptions related to cybersecurity. Information &Amp; Computer Security, 29(2), 350-364. https://doi.org/10.1108/ics-04-2020-0052

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2021). Cost benefits of using machine learning features in nids for cyber security in uk small medium enterprises (sme). Future Internet, 13(8), 186. https://doi.org/10.3390/fi13080186

Regenmortel, M. V. and Mahy, B. W. J. (2004). Emerging issues in virus taxonomy. Emerging Infectious Diseases, 10(1), 8-13. https://doi.org/10.3201/eid1001.030279

Rudner, M. (2013). Cyber-threats to critical national infrastructure: an intelligence challenge. International Journal of Intelligence and CounterIntelligence, 26(3), 453-481. https://doi.org/10.1080/08850607.2013.780552

Sáez-López, E., Pechirra, P., Costa, I., Cristóvão, P., Conde, P., Machado, A., … & Guiomar, R. (2019). Performance of surveillance case definitions for respiratory syncytial virus infections through the sentinel influenza surveillance system, portugal, 2010 to 2018. Eurosurveillance, 24(45). https://doi.org/10.2807/1560-7917.es.2019.24.45.1900140

Safety4Sea. (2019). Cyber Security challenges for the maritime industry. Erişim adresi: https://safety4sea.com/cm-cyber-security-challenges-for-the-maritime-industry/

Samtani, S., Kantarcıoğlu, M., & Chen, H. (2020). Trailblazing the artificial intelligence for cybersecurity discipline. ACM Transactions on Management Information Systems, 11(4), 1-19. https://doi.org/10.1145/3430360

Sanders, C. (2011). Practical packet analysis: using wireshark to solve real-world network problems. Network Security, 2011(8), 4. https://doi.org/10.1016/s1353-4858(11)70082-4

Sarah Kuzankah Ewuga, Zainab Efe Egieya, Adedolapo Omotosho, & Abimbola Oluwatoyin Adegbite (2024). Iso 27001 in banking: an evaluation of its implementation and effectiveness in enhancing information security. Finance &Amp; Accounting Research Journal, 5(12), 405-425. https://doi.org/10.51594/farj.v5i12.684

Sarker, I. H. (2020). Cybersecurity data science: an overview from machine learning perspective.. https://doi.org/10.20944/preprints202006.0139.v1

Sarker, I. H., Furhad, H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2(3). https://doi.org/10.1007/s42979-021-00557-0

Scalas, M., Maiorca, D., Mercaldo, F., Visaggio, C. A., Martinelli, F., & Giacinto, G. (2019). On the effectiveness of system api-related information for android ransomware detection. Computers &Amp; Security, 86, 168-182. https://doi.org/10.1016/j.cose.2019.06.004

Seatrade Maritime. (2013). Antwerp incident highlights maritime IT security risk. Erişim adresi: https://www.seatrade-maritime.com/europe/antwerp-incident-highlights-maritime-it-security-risk

SeaTrade Maritime. (2020). MSC confirms malware attack caused website outage. Erişim adresi: https://www.seatrade-maritime.com/containers/msc-confirms-malware-attack-caused-website-outage

Security Week. (2023). Japan's Nagoya Port Suspends Cargo Operations Following Ransomware Attack. Erişim adresi: https://www.securityweek.com/japans-nagoya-port-suspends-cargo-operations-following-ransomware-attack/

Sells, S. P., Smith, T. E., & Sprenkle, D. H. (1995). Integrating qualitative and quantitative research methods: a research model. Family Process, 34(2), 199-218. https://doi.org/10.1111/j.1545-5300.1995.00199.x

Senanayake, J., Kalutarage, H., & Al-Kadri, M. O. (2021). Android mobile malware detection using machine learning: a systematic review. Electronics, 10(13), 1606. https://doi.org/10.3390/electronics10131606

Sharma, P., Tiwari, S., Bijalwan, A., & Pilli, E. S. (2014). Botnet detection framework. International Journal of Computer Applications, 93(19), 29-32. https://doi.org/10.5120/16469-6159

Sihwail, R., Omar, K., & Ariffin, K. A. Z. (2018). A survey on malware analysis techniques: static, dynamic, hybrid and memory analysis. International Journal on Advanced Science, Engineering and Information Technology, 8(4-2), 1662. https://doi.org/10.18517/ijaseit.8.4-2.6827

Singgalen, Y. A., Purnomo, H. D., & Sembiring, I. (2021). Exploring msmes cybersecurity awareness and risk management : information security awareness. IJCCS (Indonesian Journal of Computing and Cybernetics Systems), 15(3), 233. https://doi.org/10.22146/ijccs.67010

Singh, T., Johnston, A. C., D'Arcy, J., & Harms, P. D. (2023). Stress in the cybersecurity profession: a systematic review of related literature and opportunities for future research. Organizational Cybersecurity Journal: Practice, Process and People. https://doi.org/10.1108/ocj-06-2022-0012

Snedaker, S. (2007). Business continuity and disaster recovery planning for it professionals.. https://doi.org/10.1016/b978-1-59749-172-3.x5000-2

Stevens, C. (2019). Assembling cybersecurity: the politics and materiality of technical malware reports and the case of stuxnet. Contemporary Security Policy, 41(1), 129-152. https://doi.org/10.1080/13523260.2019.1675258

Stine, K., Quinn, S., Witte, G., & Gardner, R. K. (2020). Integrating cybersecurity and enterprise risk management (erm).. https://doi.org/10.6028/nist.ir.8286

Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks, 10(7), 190903. https://doi.org/10.1155/2014/190903

Sviličić, B., Rudan, I., Jugović, A., & Zec, D. (2019). A study on cyber security threats in a shipboard integrated navigational system. Journal of Marine Science and Engineering, 7(10), 364. https://doi.org/10.3390/jmse7100364

Swamy, S. and Raju, K. S. (2020). An empirical study on system level aspects of internet of things (iot). IEEE Access, 8, 188082-188134. https://doi.org/10.1109/access.2020.3029847

Teti, A. and Abbott, P. (2023). Scholarship on the middle east in political science and international relations: a reassessment. PS: Political Science &Amp; Politics, 56(2), 259-264. https://doi.org/10.1017/s1049096522001378

Thatcher, J. B., Loughry, M. L., Lim, J., & McKnight, D. H. (2007). Internet anxiety: an empirical study of the effects of personality, beliefs, and social support. Information &Amp; Management, 44(4), 353-363. https://doi.org/10.1016/j.im.2006.11.007

The Jerusalem Post. (2012). Iran official: Cyber attackers target oil platforms. Erişim adresi: https://www.jpost.com/Iranian-Threat/News/Iran-official-Cyber-attackers-target-oil-platforms

The Load Star. (2020). CMA CGM gets cyber attack-hit systems back up and running. Erişim adresi: https://theloadstar.com/cma-cgm-gets-cyber-attack-hit-systems-back-up-and-running/

The Maritime Executive. (2018). Cosco Reports Cyberattack at its U.S. Operations. Erişim adresi: https://maritime-executive.com/article/cosco-reports-cyberattack-at-its-u-s-operations

Thirumaran, M., Dhavachelvan, P., Abarna, S., & Thanigaivel., K. (2010). Model-driven security assessment and verification for business services. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3427078

To, W. M. and Lee, P. K. (2018). China's maritime economic development: a review, the future trend, and sustainability implications. Sustainability, 10(12), 4844. https://doi.org/10.3390/su10124844

Torkura, K. A., Sukmana, M. I., Cheng, F., & Meinel, C. (2020). Cloudstrike: chaos engineering for security and resiliency in cloud infrastructure. IEEE Access, 8, 123044-123060. https://doi.org/10.1109/access.2020.3007338

Tsvilii, O. (2021). Cybersecurity regulation: cybersecurity certification of operational technologies. Technology Audit and Production Reserves, 1(2(57)), 54-60. https://doi.org/10.15587/2706-5448.2021.225271

Tunçbilek, M. (2024). 2022 yılında yaşanan gelişmeler doğrultusunda bilgi güvenliğinde risk yönetiminin artan önemine ilişkin bir değerlendirme.

Bilgi Ve İletişim Teknolojileri Dergisi, 6(1), 36-56. https://doi.org/10.53694/bited.1282138

Tvaronavičienė, M., Plėta, T., & Casa, S. D. (2021). Cyber security management model for critical infrastructure protection. International Scientific Conference „Contemporary Issues in Business, Management and Economics Engineering". https://doi.org/10.3846/cibmee.2021.611

Veiga, A. D., Астахова, Л. В., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—perspectives from academia and industry. Computers &Amp; Security, 92, 101713. https://doi.org/10.1016/j.cose.2020.101713

Vernon, W. (2009). The delphi technique: a review. International Journal of Therapy and Rehabilitation, 16(2), 69-76. https://doi.org/10.12968/ijtr.2009.16.2.38892

Viederytė, R. (2021). Economic implications on the basis of lithuanian maritime sector's clustering. Regional Formation and Development Studies, 118-126. https://doi.org/10.15181/rfds.v13i2.830

Volkova, M., Chmelar, P., & Sobotka, L. (2019). Machine learning blunts the needle of advanced sql injections. Mendel, 25(1), 23-30. https://doi.org/10.13164/mendel.2019.1.023

Vu, S. N. T., Stege, M., El-Habr, P. I., Bang, J., & Dragoni, N. (2021). A survey on botnets: incentives, evolution, detection and current trends. Future Internet, 13(8), 198. https://doi.org/10.3390/fi13080198

Vuorinen, J. and Tetri, P. (2012). The order machine – the ontology of information security. Journal of the Association for Information Systems, 13(9), 695-713. https://doi.org/10.17705/1jais.00306

Wang, H., Long, H., Wang, A., Liu, T., & Fu, H. (2021). Deep learning and regularization algorithms for malicious code classification. IEEE Access, 9, 91512-91523. https://doi.org/10.1109/access.2021.3090464

Warikoo, A. (2023). Perspective chapter: ransomware. Malware - Detection and Defense. https://doi.org/10.5772/intechopen.108433

Wiboonrat, M. (2008). An empirical it contingency planning model for disaster recovery strategy selection. 2008 IEEE International Engineering Management Conference. https://doi.org/10.1109/iemce.2008.4617953

Wibowo, E. J. and Ramli, K. (2022). Impact of implementation of information security risk management and security controls on cyber security maturity (a case study at data management applications of xyz institute). Jurnal Sistem Informasi, 18(2), 1-17. https://doi.org/10.21609/jsi.v18i2.1146

Widodo, N. P., Permadi, D. A., Ihsan, A., & Kusuma, G. J. (2021). Development of comprehensive fire and explosion risk assessment on coal reclaim tunnel using monte carlo simulation and risk matrix method. Engineering Reports, 4(4). https://doi.org/10.1002/eng2.12476

Windward. (2022). AIS Spoofing: New Technologies for New Threats. Erişim adresi: https://windward.ai/blog/ais-spoofing-new-technologies-for-new-threats/

Wiseman, Y. (2014). Steganography based seaport security communication system. Advanced Science and Technology Letters. https://doi.org/10.14257/astl.2014.46.63

Youm, H. Y. (2017). An overview of security and privacy issues for internet of things. IEICE Transactions on Information and Systems, E100.D(8), 1649-1662. https://doi.org/10.1587/transinf.2016ici0001

Zainuddin, N., Yusuff, R. C. M., & Samy, G. N. (2020). Risk evaluation using nominal group technique for cloud computing risk assessment in healthcare. International Journal on Advanced Science, Engineering and Information Technology, 10(1), 106-111. https://doi.org/10.18517/ijaseit.10.1.10169

Zajac, J. B. P. (1994). Applied cryptography: protocols, algorithms, and source code in c. Computers &Amp; Security, 13(3), 217-218. https://doi.org/10.1016/0167-4048(94)90072-8

Zammani, M., Razali, R., & Singh, D. (2021). Organisational information security management maturity model. International Journal of Advanced Computer Science and Applications, 12(9). https://doi.org/10.14569/ijacsa.2021.0120974

Zarei, J. and Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: a case study of iran. Risk Management and Healthcare Policy, 75. https://doi.org/10.2147/rmhp.s99908

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. IEEE Communications Surveys &Amp; Tutorials, 15(4), 2046-2069. https://doi.org/10.1109/surv.2013.031413.00127

Zhang, J., Wang, M. M., Xia, T., & Wang, L. (2020). maritime iot: an architectural and radio spectrum perspective. IEEE Access, 8, 93109-93122. https://doi.org/10.1109/access.2020.2990830

Zhang, L., Liu, P., Choi, Y., & Chen, P. (2023). Semantics-preserving reinforcement learning attack against graph neural networks for malware detection. IEEE Transactions on Dependable and Secure Computing, 20(2), 1390-1402. https://doi.org/10.1109/tdsc.2022.3153844

Zhao, Z. D., Huang, Z., Huang, L., Liu, H., & Lai, Y. (2014). Scaling and correlation of human movements in cyberspace and physical space. Physical Review E, 90(5). https://doi.org/10.1103/physreve.90.050802

ÖZGEÇMİŞ

ÖĞRENİM BİLGİSİ:

- Doktora: Gedik Üniversitesi Lisansüstü Eğitim Enstitüsü/Uluslararası Ticaret Doktora Programı – 2024
- Yüksek Lisans: Gedik Üniversitesi/Sosyal Bilimler Enstitüsü/Siyaset Bilimi ve Kamu Yönetimi – 2018
- Lisans: Anadolu Üniversitesi/İşletme Fakültesi/İşletme - 2013

MESLEKİ DENEYİM:

- 2020 – Halen: Genel Müdür – Vitriol Bilişim Ltd. Şti.
- 2020 – 2023: Genel Yayın Yönetmeni – Cloud7
- 2020 – 2023: CISO – 24 Solutions Turkey
- 2016 – 2020: BT Güvenliği & Operasyon Müdürü – 24 Solutions Turkey
- 2014 – 2016: Ülke Müdürü – Mile2
- 2012 – 2014: Genel Yayın Yönetmeni – T3
- 2011 – 2012: Linux Sistem Yöneticisi – AltınNet
- 2009 – 2011: Yazı İşleri Müdürü – BYTE
- 2008 – 2009: Yazılım Editörü – PC World
- 2006 – 2008: Oyun Editörü – GamePro
- 2005 – 2006: Oyun Programcısı – Mistic Software Inc.
- 2003 – 2004: Oyun Programcısı – Aedon Games

TEZDEN TÜRETİLEN YAYINLAR, SUNUMLAR, PATENTLER:

- Keleştemur, S. A., Atatüre, S., Elmas, G., "A Proposal For A Monte Carlo Simulation-Based Risk Framework With Optimal Cost Balance For The Maritime Industry", Ekonomi, İşletme ve Maliye Araştırmaları Dergisi, Kabul Tarihi: 16 Temmuz 2024, İstanbul, Türkiye.
- Keleştemur, S.A., Elmas G., Özdemir, İ., Köseoğlu, A.M., "Analysis of Cyber Risk Management Frameworks for The Maritime Industry", Piri Reis Üniversitesi - 14th International Exergy, Energy, and Environment Symposium, 24-27 Aralık 2024, Istanbul, Türkiye.
- Keleştemur, S.A., "Modern Korsanlık: Siber Saldırı ile Gemi Kontrolü ve Rota Değişiklikleri", Piri Reis Üniversitesi - Deniz Hukukunda Korsanlık ve Güvenlik, 26 Nisan 2024, İstanbul, Türkiye.

ULUSAL HAKEMLİ DERGİLERDE YAYIMLANAN MAKALELER:

- Keleştemur, A., Koldemir, B., Yapıcı, M., "Deniz Taşımacılığında Siber Güvenliği Tehdit Eden Unsurlar ve Koruma Önlemleri Üzerine Bir Çalışma", Dokuz Eylül Üniversitesi - III. Ulusal Liman Kongresi, 2017, İzmir, Türkiye.

ULUSAL/ULUSLARARASI KİTAPLARDAKİ BÖLÜMLER

- Kolektif. (2023). İstihbarat Teknolojileri, Bölüm adı: Siber İstihbarat Teknolojisi, Kamer Yayınları, Editör: Sait Yılmaz, Basım Sayısı: 1, Sayfa Sayısı: 385, Bölüm Sayfaları: 140-185, ISBN: 9786257073547.
- Keleştemur, A. (2015). Siber İstihbarat, Level, Basım Sayısı: 1, Sayfa Sayısı: 472, ISBN: 9786056567926.
- Keleştemur, A. (2012). Windows 8, Kodlab, Basım Sayısı: 1, Sayfa Sayısı: 172, ISBN: 9786054205646.
- Keleştemur, A. (2011). Pardus 2011, Kodlab, Basım Sayısı: 1, Sayfa Sayısı: 226, ISBN: 9786054205493.
- Keleştemur, A., (2011). Ubuntu, Kodlab, Basım Sayısı: 1, Sayfa Sayısı: 310, ISBN: 9786054205554.

PROJELERDE YAPTIĞI GÖREVLER:

- 2023 – 2024: ISECOM/ OSSTMM – ARGE Takım Üyesi
- 2022 – 2023: AlmaLinux OS – Program Yöneticisi
- 2017 – 2019: Uluslararası Siber Güvenlik Federasyonu – Başkan Yardımcısı
- 2011 – 2012: Türkiye Bilişim Derneği İstanbul Şubesi – Açık Kaynak Çalışma Grubu Başkanı
- 2008 – 2010: Türkiye Bilişim Güvenliği Derneği – Başkan Yardımcısı

KURS / SEMİNER / SERTİFİKA:

- CompTIA Advanced Security Practitioner (CASP+)
- CompTIA PenTest+
- Mile2 Certified Penetration Testing Engineer (CPTE)
- Mile2 Certified Secure Web Application Engineer (CSWAE)
- Mile2 Certified Professional Ethical Hacker (CPEH)
- CWL Multi-Cloud Red Teaming Analyst (MCRA)
- Sophos Certified Engineer (SCE)
- Sızma Testi Uzmanı (TSE)
- ISO 27001 Baş Denetçisi Sertifikası