Jurnal Ilmiah Universitas Batanghari Jambi **e-ISSN**: 2549-4236, **p-ISSN**: 1411-8939
Lembaga Penellitian dan Pengabdian kepada Masyarakat
Vol 23, No 3 (2023): Oktober, 2739-2748
DOI: 10.33087/jiubj.v23i3.3839

Penerapan Keamanan Siber pada Sistem Transportasi Laut

Sahrudin, Muhamad Bahrul Ulum
Universitas Esa Unggul
Correspondence: aloel.ku@student.esaunggul.ac.id, m.bahrul_ulum@esaunggul.ac.id

Abstrak. Sistem transportasi laut semakin bergantung pada teknologi komputasi dan komunikasi, Informasi Teknologi (IT) dan Operasional Teknologi (OT) harus bekerja sama untuk melindungi informasi dan merancang keamanan untuk kegiatan kriminal yang disebabkan oleh serangan siber. Sistem tahapan proses dan penilaian keamanan siber untuk kapal diperlukan agar kerentanan sistem transportasi laut terhadap serangan siber dapat diukur secara akurat dan efektif. Menggunakan *framework* NIST, CIA model dan *Risk Assessment Matrix* (RAM) untuk identifikasi dan pengukuran merupakan kunci terpenting dalam proses penilaian keamanan siber pada sistem transportasi laut. Dengan ruang lingkup analisis pada infrastruktur kapal meliputi sistem jaringan, komputer, perangkat komunikasi kapal, pengujian, dan penilaian.

Kata kunci : framework NIST; CIA model; risk assessment; keamanan siber; sistem transportasi laut

Abstract. *Marine transportation systems are increasingly dependent on computing and communication technologies, Information technology (IT) and operational technology (OT) must work together to protect information and design security against criminal activity from cyberattacks. A system of process stages and cybersecurity assessments for ships is necessary so that the vulnerability of marine transport systems to cyberattacks can be measured accurately and effectively. Using the framework NIST, The CIA model and Risk Assessment Matrix (RAM) for identification and measurement is the most important key in the cybersecurity assessment process of marine transport systems. With the scope of analysis on vessel infrastructure including network systems, computers, ship communication devices, testing, and assessment.*

Keywords **:** *framework NIST; he CIA model; risk assessment; Cybersecurity; marine transportation system*

PENDAHULUAN

Sistem transportasi laut bergantung pada komputasi dan komunikasi, memanfaatkan teknologi dalam bentuk digitalisasi, konektivitas, dan integrasi. Kemajuan teknologi internet berdampak pada pola komunikasi, dan kapal sudah menggunakan teknologi satelit untuk mempercepat jalur komunikasi dengan pemilik kapal dan otoritas terkait, mengirimkan pesan dan informasi baik ke kapal maupun pihak di darat. Dengan terkoneksinya kapal pada jaringan internet, maka tingkat risiko kerentanan akibat kejahatan siber semakin meningkat. Pada Februari 2019, sebuah kapal *Deep Draft* dalam pelayaran internasional menuju pelabuhan *New York* dan *New Jersey* melaporkan bahwa mereka mengalami insiden serangan siber yang signifikan dan berdampak pada jaringan kapal. Sebuah tim ahli siber yang dipimpin oleh US *Coast Guard* menanggapi dan melakukan analisis terhadap jaringan kapal dan sistem kontrol. Hasil temuan menyimpulkan bahwa *malware* secara signifikan menurunkan fungsionalitas pada sistem komputer *onboard*, sedangkan sistem kontrol kapal tidak terpengaruh. Dari kejadian tersebut ditemukan kerentanan bahwa kapal beroperasi tanpa langkah-langkah keamanan siber yang efektif dapat mengekspos sistem kontrol kapal yang kritis terhadap kerentanan signifikan (US Coast Guard, 2019).

Perkembangan sektor industri maritim yang semakin bergerak menuju tingkat layanan digital pada pelabuhan dan kapal *autonomous*, membutuhkan protokol keamanan siber untuk peningkatan langkah-langkah perlindungan. Pelabuhan atau kapal berisiko terkena serangan siber jika sistem informasi utama tidak dilindungi secara memadai (Farah et al., 2022). Bagaimana langkah-langkah keamanan siber yang harus dilakukan kapal dalam mengeksplorasi fasilitas navigasi kapal yang saling berhubungan dan dapat menjadi ancaman siber, bagaimana *hacker* membuat sinyal GPS (Lee et al., 2017). Pada jaringan VSAT yang tidak memiliki enkripsi lapisan dasar dan VSAT menjadi ancaman baru terhadap kapal yang dapat di eksploitasi oleh berbagai serangan siber (Pavur et al., 2020). Anomali dalam pesan NMEA dapat disebabkan oleh *cyberattack*, data NMEA membawa informasi yang sangat penting untuk beberapa fungsi navigasi, seperti

penghindaran tabrakan (Amro et al., 2022). Sehingga diperlukan metode penilaian risiko yang didasarkan pada identifikasi kelompok serangan yang berpotensial, kerentanan komponen sistem, skenario serangan dan peringkat berdasarkan pedoman khusus (Bolbot et al., 2020). Penggunaan *Framework* NIST dapat mendukung organisasi dalam pendekatan penilaian risiko, dengan membantu memahami pendekatan yang efektif dalam mengelola potensi risiko siber. *Framework* CIA menjadi bagian dari penilaian kerentanan OT *systems onboard* yang berfokus pada keteresediaan dan integritas data. RAM (*Risk Assessment Matrix*) merupakan penilaian risiko yang mengukur dampak peristiwa keamanan siber berdasarkan kategori tertentu (BIMCO, 2021). Menurut Surat Edaran Direktur Jenderal Perhubungan Darat NomoriSE.35 Tahun 2020, sistem informasi transportasi laut yang memiliki kerentanan ancaman jaringan maya (*cyberattack*) meliputi hal-hal sebagai berikut: sistem anjungan atau ruang navigasi, sistem manajemen penanganan muatan, manajemen tenaga penggerak dan permesinan serta sistem kontrol daya, sistem kontrol akses, sistem pelayanan dan penanganan penumpang, jaringan publik untuk penumpang, sistem administrasi dan kesejahteraan karyawan, dan sistem komunikasi. Sistem tahapan proses dan penilaian risiko keamanan siber (*cyber risk assessment*) pada kapal, bagian dari safety committee. Sehingga kerentanan sistem transportasi laut pada infrastruktur kapal terhadap serangan siber dapat diukur secara akurat dan efektif. Dampak penilaian risiko keamanan siber pada sistem transportasi laut yang belum terukur, mengakibatkan pemilik kapal (*shipowner*) tidak dapat memberikan kepastian proteksi keamanan siber terhadap penyewa kapal (*charter*). Maka perlu dilakukan analisis kondisi infrastruktur kapal meliputi: jaringan kapal, pengujian jaringan, keamanan jaringan dan perangkat kapal, serta membuat rekomendasi penilaian keamanan, sebagai langkah dalam penerapan keamanan siber sistem transportasi laut pada infrastruktur kapal.

METODE

Penelitian dilakukan di kapal MV Oceanic Success milik PT Indobaruna Bulk Transport (IBT), dengan lokasi kantor pusat di gedung The Prominence Office Tower Lt. 19 Jl. Jalur Sutera Barat Kav. 15 Alam Sutera Tangerang 15143. Objek Penelitian yang dilakukan di IBT mengenai penerapan keamanan siber pada sistem transportasi laut pada armada kapal milik dengan angkutan khusus semen curah. Penelitian ini di bangun untuk melakukan evaluasi tingkat keamanan siber pada armada kapal milik IBT dalam mengantisipasi ancaman serangan siber pada sistem transportasi laut. Pada penelitian ini sistem penerapan keamanan dan desain bangunan yang akan di bangun dibuat dengan tiga metode yaitu: *framework* NIST, CIA model triad dan *risk assessment*. Metode ini digunakan dalam penerapan konstruksi keamanan siber yang terdiri dari pedoman, rekomendasi, spesifikasi teknis, dan laporan untuk mendukung keamanan dan privasi pada sistem.

HASIL

Analisa Metode Keamanan

Dalam penerapan keamanan siber di kapal milik IBT, analisis dilakukan dengan tiga metode yaitu: *framework* NIST Gambar 1, CIA model, dan *risk assessment*.

Sumber: data olahan

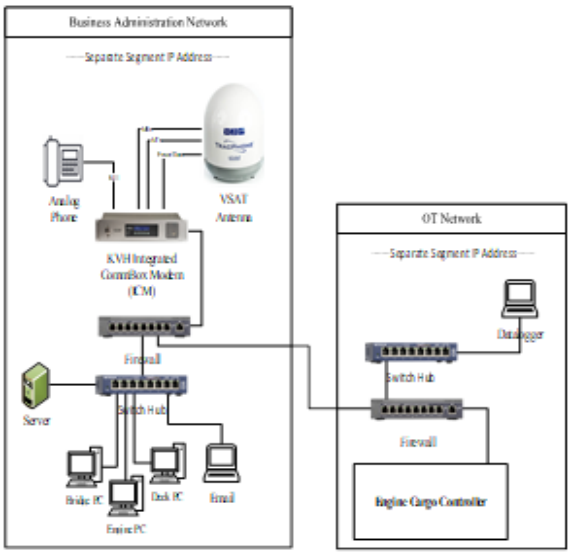
Gambar 1
***Framework* NIST**

Karakteristik dan Jenis Firewall

Dalam implementasi keamanan jaringan sistem transportasi laut infrastruktur kapal milik IBT digunakan firewall yang mempunyai karakteristik sesuai kebutuhan kapal dan dilihat dari segi keamanan, diantaranya: (1) *Firewall* diletakkan di antara VSAT dan jaringan operasional kerja; (2) *Firewall* diletakkan di antara operasional kerja dan operasional kapal; (3) Informasi yang keluar atau masuk harus melalui *firewall*; (4) Dapat melakukan fungsi filtering dan penutupan akses port; (5) Mendukung VLAN; dan (6) *User Interface* bisa melalui terminal maupun GUI. Berdasarkan karakteristik di atas pada kapal milik IBT menggunakan jenis firewall small business dari merk Netgear dan Cisco.

Pemasangan Perangkat Firewall dan ICM

Tahap selanjutnya pemasangan perangkat pada jaringan operasional kerja dan operasional kapal Gambar 2 dimana setiap jaringan memiliki segment IP address yang berbeda. Di antaranya *business network firewall* Gambar 3, OT *network firewall*



Sumber: data olahan

Gambar 2
Topologi Jaringan *Firewall*

Sumber: data olahan

Gambar 3
Business Network Firewall

Konfigurasi IP Address Pada Firewall Dan ICM

Setelah dilakukan pemasangan firewall pada jaringan sistem transportasi laut infrastruktur kapal, langkah selanjutnya melakukan konfigurasi IP address pada masing-masing firewall sesuai dengan Tabel 1 Proses konfigurasi IP address pada firewall Gambar 4 dan ICM 5ambar 5.

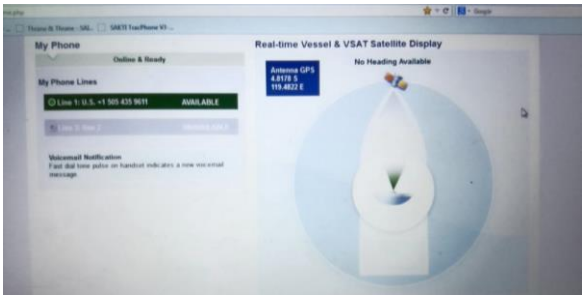
Tabel 2
IP *Address*

Device Name	Interface	IP Address	Subnetmask	Gateway
ICM VSAT	Modem	192.168.8.1	N/A	N/A
IT Router	Fa0/0	192.168.8.1	255.255.255.0	N/A
	Fa0/1	192.168.0.1	255.255.255.0	N/A
OT Router	Fa0/0	192.168.0.253	255.255.255.0	N/A
	Fa0/1	192.168.2.253	255.255.255.0	N/A

Sumber: data olahan

Sumber: data olahan

Gambar 4
Konfigurasi IP *Address Firewall*



Sumber: data olahan

Gambar 5
Konfigurasi IP *Address* VSAT ICM

Konfigurasi Port, Outbound, Inbound Pada Firewall

Setelah dilakukan konfigurasi IP address pada *firewall*, langkah selanjutnya melakukan konfigurasi *service port firewall* Gambar 6, *outbound*, dan *inbound firewall* Gambar 7. Adapun akses port dan IP address dilakukan pembatasan sesuai pada Tabel 3 dan Tabel 4.

Tabel 3
Akses *Service Port*

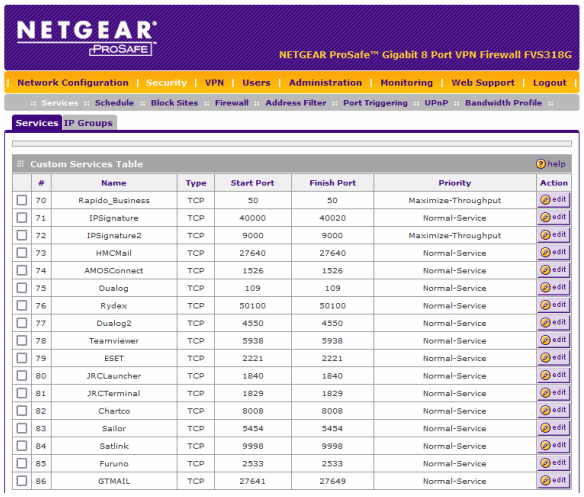
Port	Service	Status
27461-27469	GTMAIL	Open
50	Rapido_Business	Open
4000-40020	IPSignature	Open
9000	IPSignature2	Open
27640	HMCMail	Open
1526	AMOSConnect	Open
109	Dualog	Open
50100	Rydex	Open
4550	Dualog2	Open
5938	Teamviewer	Open
2221	Eset	Open
1840	JRCLauncher	Open
1829	JRCTerminal	Open
8008	Chartco	Open
5454	Sailor	Open
9998	Satlink	Open
2533	Furuno	Open

Sumber: data olahan

Tabel 4
Akses IP *Address*

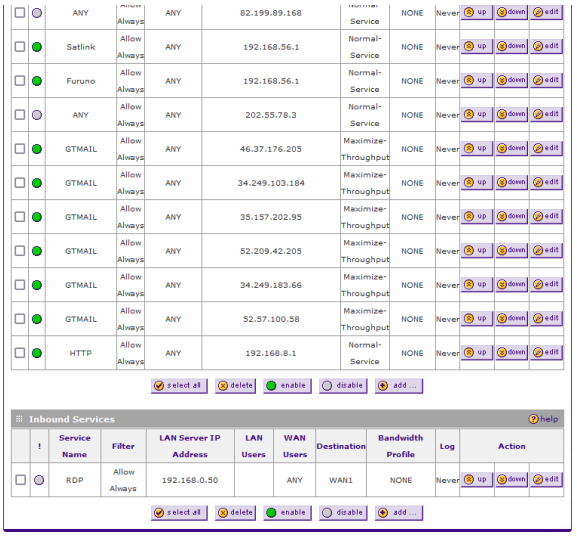
IP Address	Service	Status
46.37.176.205		Open
34.249.103.184		Open
35.157.202.95		Open
52.209.42.205	GTMailPlus	Open
52.57.100.58		Open
34.249.103.66		Open
34.249.183.66		Open
192.168.8.1	KVH	Open
192.168.56.1	Fleet Broandband	Open

Sumber: data olahan



Sumber: data olahan

Gambar 6
Service Port Firewall



Sumber: data olahan

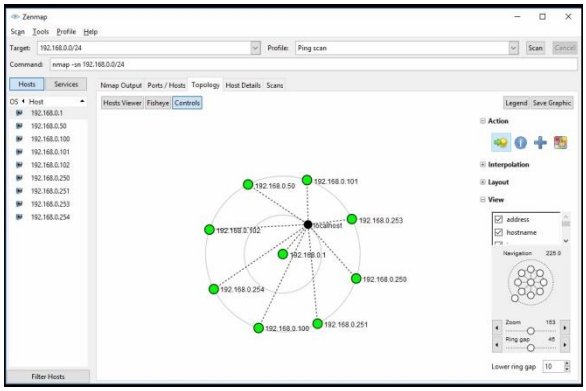
Gambar 7
Outbound* dan *Inbound Firewall

Pengujian Keamanan Siber

Langkah selanjutnya proses pengujian keamanan siber terhadap jaringan operasional kerja dan operasional kapal.

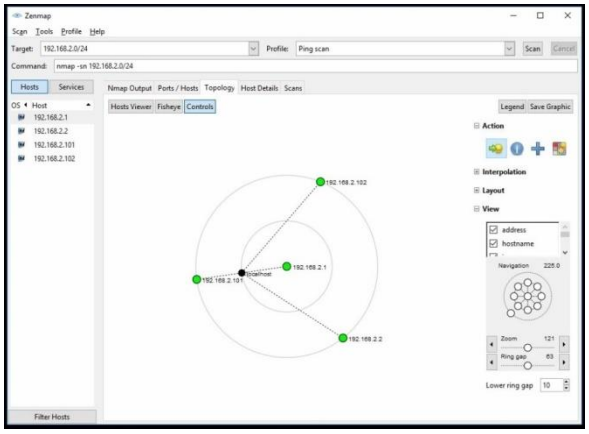
Mapping Network

Pengujian pertama melakukan *mapping network* menggunakan aplikasi nmap pada jaringan sistem transportasi laut.



Sumber: data olahan

Gambar 8
***Mapping Network* Operasional Kerja**



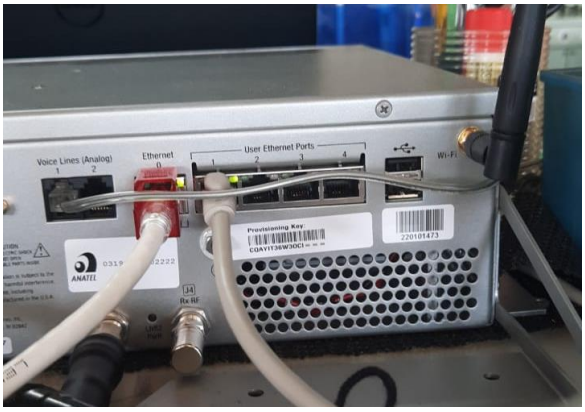
Sumber: data olahan

Gambar 9
***Mapping Network* Operasional Kapal**

Hasil *mapping network* pada Gambar 8 dan Gambar 9. Terdapat sembilan perangkat terhubung di jaringan operasional kerja dan empat perangkat yang terhubung di jaringan operasional kapal. Masing-masing jaringan memiliki IP *address* dengan *segment* berbeda yaitu: 192.168.0.0/24 dan 192.168.2.0/24

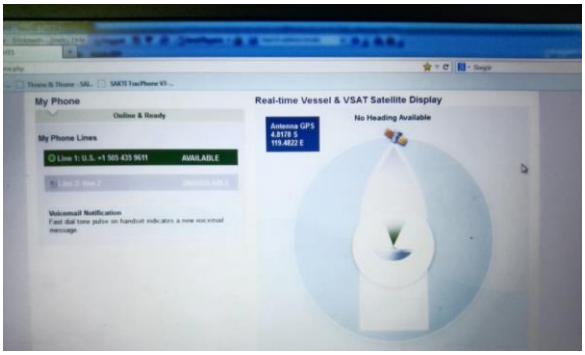
Akses VSAT

Langkah kedua melakukan akses melalui jaringan operasional kerja ke *portal* ICM VSAT Gambar 10 dan Gambar 11, dengan menggunakan aplikasi *browser* pada laptop.



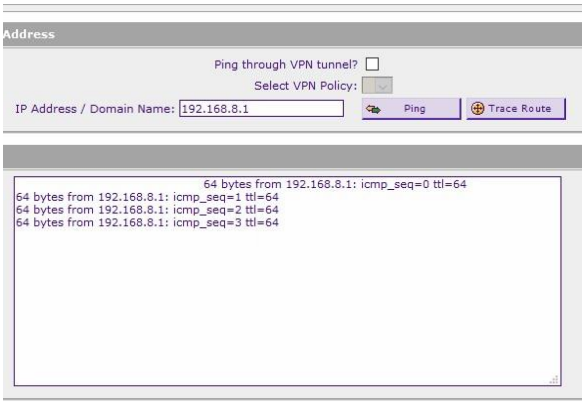
Sumber: data olahan

Gambar 10
Koneksi LAN ICM KVH



Sumber: data olahan

Gambar 11
Portal KVH ICM



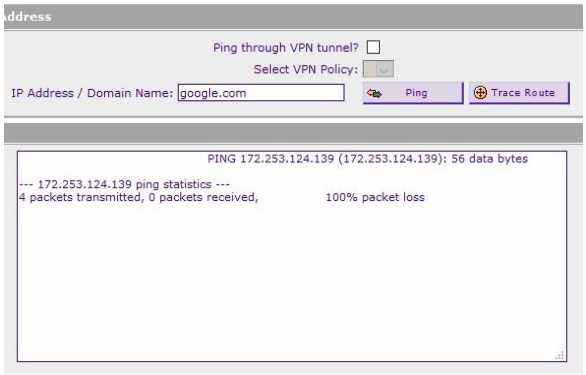
Sumber: data olahan

Gambar 12
Hasil *Ping* ke ICM VSAT

Gambar 12, merupakan hasil *ping* melalui *business network firewall* ke perangkat ICM VSAT, hasil jaringan terkoneksi dengan baik.

Akses Internet

Langkah ketiga melakukan *ping* ke jaringan internet melalui *business network firewall*.



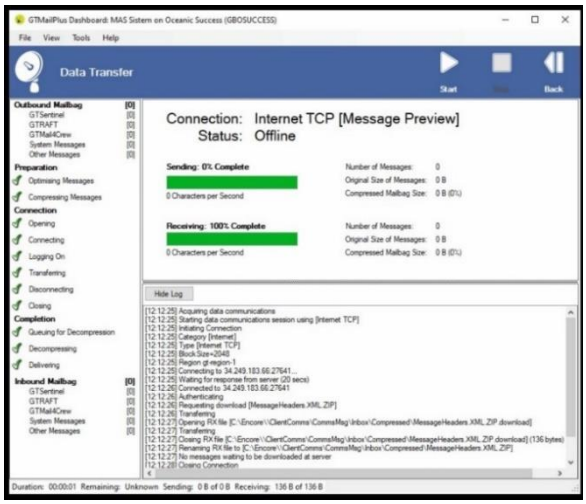
Sumber: data olahan

Gambar 13
Hasil *Ping* ke Internet

Gambar 13, merupakan hasil *ping* melalui *business network firewall* ke jaringan internet google.com, hasil jaringan tidak dapat terkoneksi.

Akses *Email*

Langkah keempat melakukan pengiriman dan penerimaan *email* menggunakan aplikasi pihak ketiga GTMailPlus pada laptop kapal.



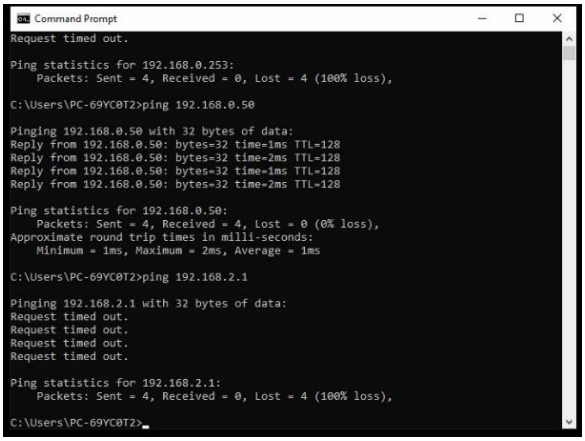
Sumber: data olahan

Gambar 14
Hasil Pengiriman *Email*

Gambar 14, merupakan hasil pengiriman dan penerimaan *email* menggunakan GTMailPlus melalui *business network firewall*, hasil jaringan dapat terkoneksi dengan baik.

Akses Jaringan Operasional Kerja

Langkah kelima melakukan *ping* dari jaringan operasional kerja ke operasional kapal.



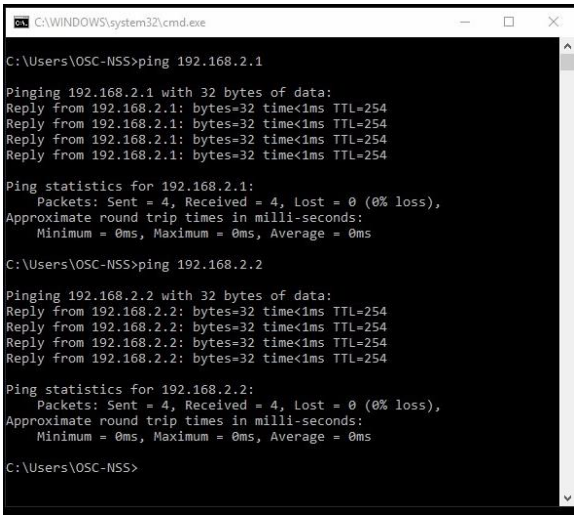
Sumber: data olahan

Gambar 15
Hasil *Ping* Operasional Kerja

Gambar 15, *ping* ke IP *address* 192.168.0.50 status berhasil, *ping* ke IP *address* 192.168.2.1 status tidak berhasil, hasil ditemukan operasional kerja tidak dapat terhubung secara langsung ke operasional kapal.

Akses Jaringan Operasional Kapal

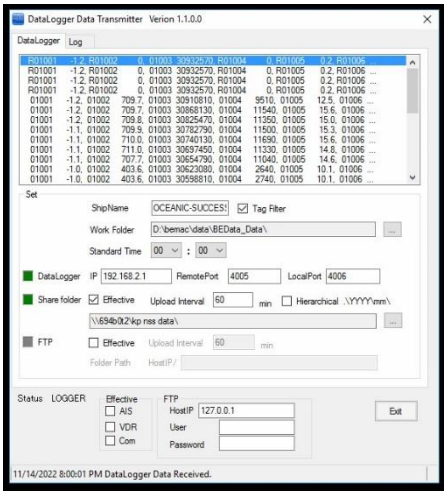
Langkah keenam melakukan *ping* dari jaringan operasional kapal ke jaringan operasional kerja.



Sumber: data olahan

Gambar 16
Hasil *Ping* Operasional Kapal

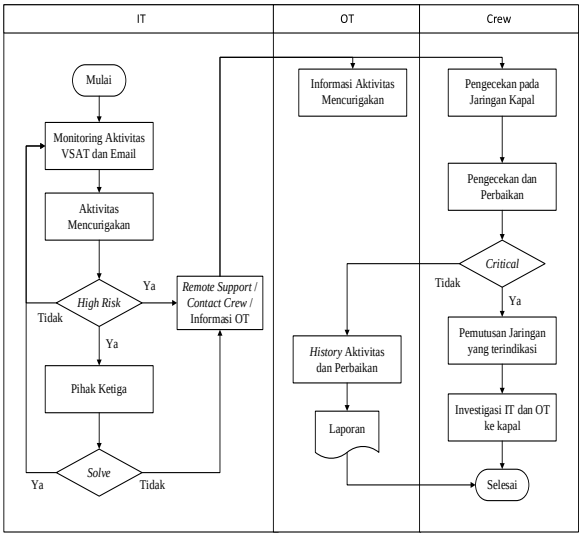
Gambar 16, *ping* ke IP address 192.168.2.1 berhasil, hasil pada jaringan operasional kapal berhasil terkoneksi sesama jaringannya, gambar 17 merupakan aplikasi datalogger pada jaringan operasional kapal.



Sumber: data olahan

Gambar 17
***Datalogger* Operasional Kapal**

Monitoring Keamanan Siber



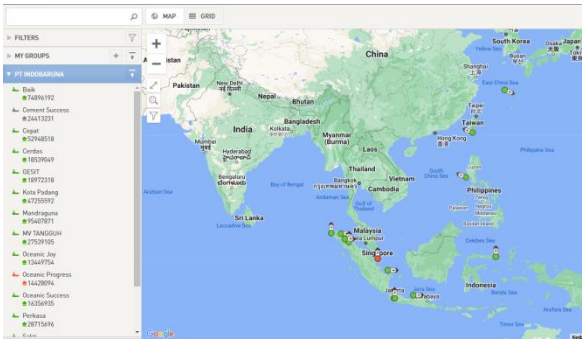
Sumber: data olahan

Gambar 18
***Activity* Diagram *Monitoring* Keamanan Siber**

Activity diagram pada gambar 18 menjelaskan alur aktivitas monitoring keamanan siber yang dilakukan IT, OT dan *crew* pada sistem transportasi laut infrastruktur kapal. Melakukan monitoring aktivitas pada jaringan VSAT dan *email*, supporting pihak ketiga dalam monitoring aktivitas mencurigakan, informasi ke pihak OT, *crew*, dan juga melakukan perbaikan maupun investigasi lanjutan.

Monitoring Traffic Komunikasi VSAT

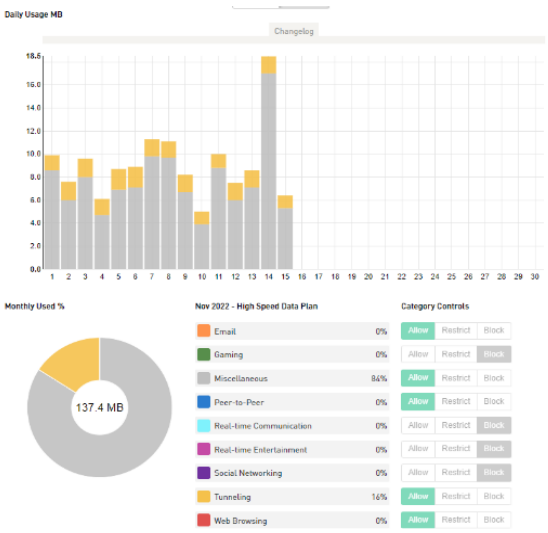
Monitoring traffic komunikasi VSAT menggunakan portal pihak ketiga milik KVH, *monitoring* yang dilakukan adalah *traffic* pengiriman dan penerimaan data. Jika terdapat ketidaksesuaian maka IT dan pihak ketiga akan melakukan investigasi dan rekonfigurasi *firewall* VSAT. Apabila masih mengalami ketidaksesuaian, akan dilakukan rekonfigurasi *firewall* di kapal pada area operasional kerja.



Sumber: data olahan

Gambar 19
Posisi Kapal dan Status VSAT

Pada gambar 19, merupakan tampilan posisi kapal dan status koneksi VSAT secara *realtime.*



Sumber: data olahan

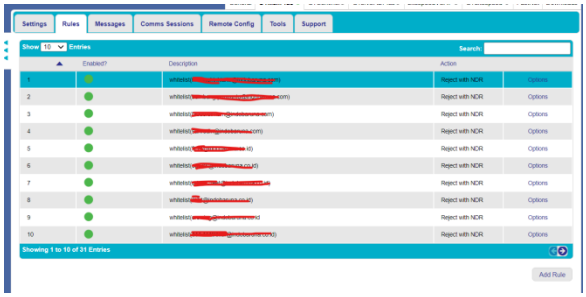
Gambar 20
***Traffic Monitoring* VSAT**

Pada gambar 20, merupakan informasi *monitoring traffic* pengiriman dan penerimaan data melalui jaringan VSAT dan juga pengaturan *firewall* berdasarkan *category control*.

Monitoring Traffic Komunikasi Email

Monitoring traffic email menggunakan portal pihak ketiga milik GTMailPlus, monitoring yang dilakukan adalah *traffic*

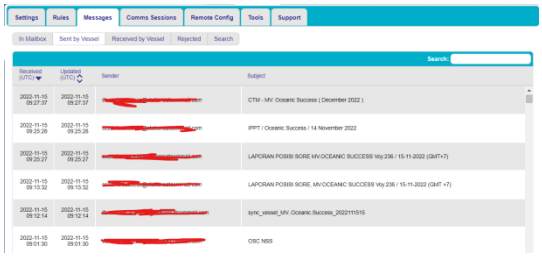
pengiriman dan penerimaan *email* dari kapal maupun pihak eksternal. Pada komunikasi *email* dilakukan pembatasan terhadap pihak eksternal yang mengirim informasi *email* ke kapal.



Sumber: data olahan

Gambar 21
Rules Email

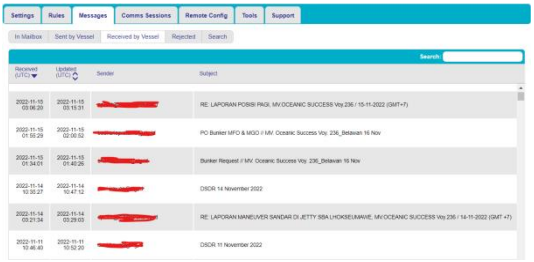
Pada gambar 21, merupakan pembuatan akses *rules whitelist* di mana hanya *email* terdaftar yang bisa mengirimkan berita ke kapal.



Sumber: data olahan

Gambar 22
Informasi *Email* Keluar

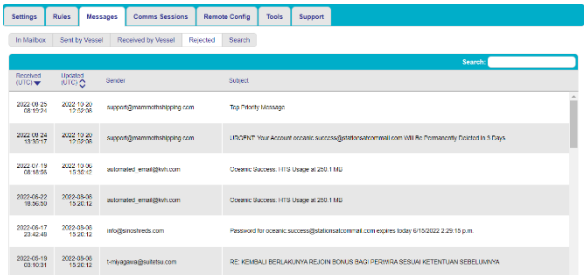
Pada gambar 22, merupakan informasi pengiriman *email* keluar dari kapal ke pihak eksternal.



Sumber: data olahan

Gambar 23
Informasi *Email* Terima

Pada gambar 23, merupakan informasi penerimaan *email* ke kapal dari pihak eksternal.



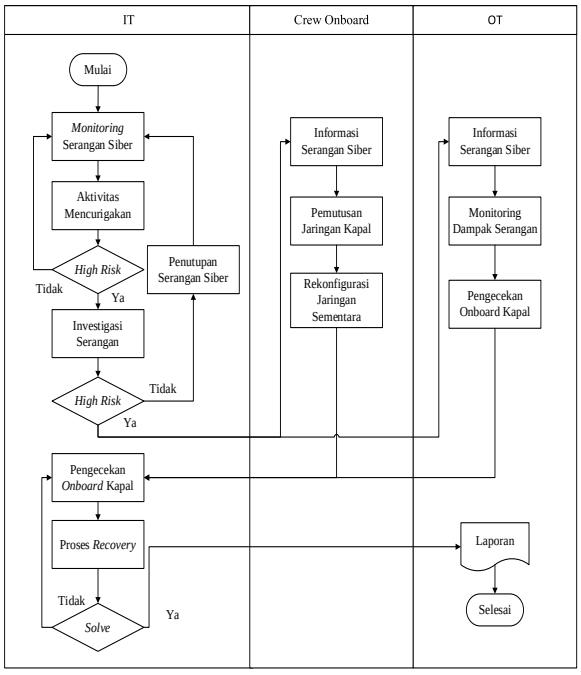
Sumber: data olahan

Gambar 24
Informasi *Email* Ditolak

Pada gambar 24, merupakan informasi *email* yang ditolak sebelum di kirim ke kapal dari pihak eksternal. Di mana pada *firewall* GTMailPlus mempunyai fitur *filtering email spam* dan *phising*.

Recovery Serangan Siber

Proses *recovery* diperlukan setelah serangan siber terhadap sistem transportasi laut infrastruktur kapal terjadi, agar jaringan operasional kerja dan operasional kapal kembali pulih dari kerusakan sistem akibat serangan siber.



Sumber: data olahan

Gambar 25
***Activity* Diagram *Recovery* Serangan Siber**

Activity diagram pada gambar 25 menjelaskan aktivitas monitoring serangan siber dan proses *recovery* yang dilakukan IT, OT, dan *crew* sehingga sistem transportasi laut pada

infrastruktur kapal dapat dipulihkan dan berfungsi normal.

1. IT melakukan monitoring akan aktivitas mencurigkan, melakukan penutupan keamanan jika termasuk kategori *low* dan *medium risk*.
2. Jika kategori *high risk* akan menginformasikan ke *crew* maupun OT, *crew* melakukan langkah pemutusan koneksi jaringan berdasarkan arahan dari IT
3. OT melakukan monitoring akibat dampak serangan siber, kemudian melakukan pengecekan secara *onboard* bersama IT.
4. IT melakukan proses *recovery* sistem transportasi laut yang terdampak dan mengembalikan ke fungsi normal.

Klasifikasi Serangan Siber

Setelah dilakukan identifikasi dan Pengujian kerentanan siber selanjutnya pengelompokan klasifikasi serangan siber pada perangkat sistem transportasi laut infrastruktur kapal berdasarkan CIA model Gambar 26 untuk memudahkan IT dan OT dalam analisis keamanan. Berikut klasifikasi serangan dan dampak keamanan pada perangkat sistem transportasi laut infrastruktur kapal Tabel 5.

Sumber: data olahan

Gambar 26
CIA Model *Triad*

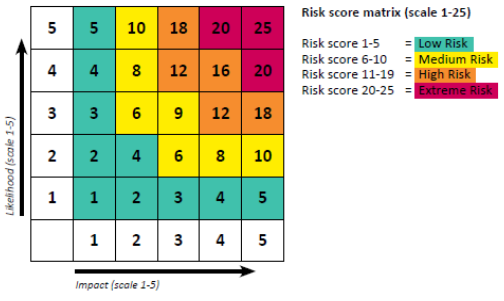
Tabel 5
Klasifikasi Serangan Siber

No	Kategori	Serangan	Kerentangan	Dampak C	Dampak I	Dampak A
1	*Automatic Identification System* (AIS)	*Spoofing* *Frequency mapping* *Timming attack*	*Open system* *Lack of encryption algorithms*	●	○	●
2	Radar dan Radio *Communication*	*Spoofing using* GPS	*Insufficient data protection* *Autonomous vessels* *Vessel identity theft* (GPS *spoofing*)	●	●	●
3	*Propulsion Management* (PM) / *Power Control Systems* (PCS)	*Spoofing*	*Usage of digital systems* *Integration with communications equipment*	○	○	●
4	*Access to System* (AS)	*Spear-phishing technique* *Key loggers installation* *Malware attack* *Viknok Trojan*	*Insufficient e-mail protection* *Using external devices*	●	○	○
5	*Alarm System* (A1.S)	*General attacks*	*Equipment connected to the* internet	●	○	●
6	*Cargo Management Systems* (CMS)	*Spoofing* *Man-in-the-middle attack*	*Shipment-tracking tools* *The tracking is via the* internet	●	●	○
7	*Bridge Systems* (BS)	*DoS attack*	*Using of removable media for update*	○	○	●
8	*Passenger servicing and Management Systems* (PCMS)	*DoS attack* *Spoofing* *Malware attack*	*Digital systems* *Access control*	●	●	●
9	*Passenger Facing Public Networks* (PPN)	*All kinds of cyber-attacks*	Internet *connection*	●	●	●
10	*Administrative and crew welfare systems* (ACWS)	*All kinds of cyber-attacks*	*Computer networks of the ship connected to the* internet	●	●	●

Sumber: data olahan

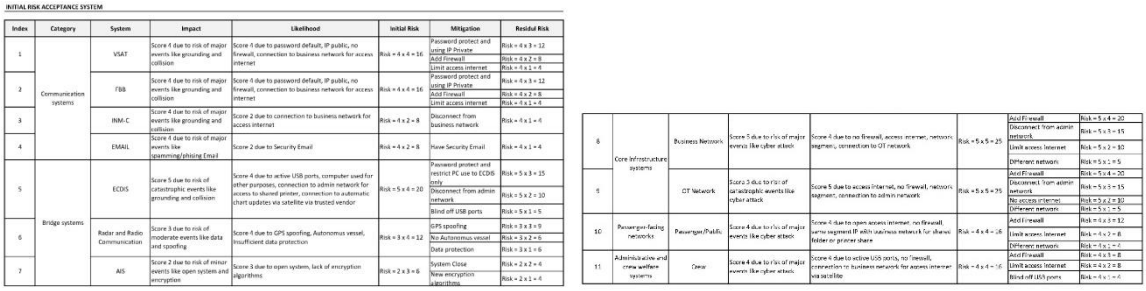
Internal Risk Assessment
Pengukuran Risk Assessment

Setelah tahap identifikasi, pengujian, dan klasifikasi keamanan siber selesai. Langkah selanjutnya melakukan pengukuran risiko menggunakan metode *Risk Assessment Matrix* (RAM) Gambar 27. Berdasarkan *initial risk acceptance system* gambar 28 yang sudah ditentukan oleh IT dan OT.



Sumber: data olahan

Gambar 27
Risk Assessment Matrix (RAM)



INITIAL RISK ACCEPTANCE SYSTEM

Index	Category	System	Impact	Likelihood	Initial Risk	Mitigation	Residual Risk
1	Communication systems	VSAT	Score 4 due to risk of major events like grounding and collision	Score 3 due to password default, IP public, no firewall, connection to business network for access internet	Risk = 4 x 4 = 16	Password protect and using IP Private	Risk = 4 x 3 = 12
						Add Firewall	Risk = 4 x 2 = 8
						Limit access internet	Risk = 4 x 1 = 4
2		FBB	Score 4 due to risk of major events like grounding and collision	Score 4 due to password default, IP public, no firewall, connection to business network for access internet	Risk = 4 x 4 = 16	Password protect and using IP Private	Risk = 4 x 3 = 12
						Add Firewall	Risk = 4 x 2 = 8
						Limit access internet	Risk = 4 x 1 = 4
3		INM-C	Score 4 due to risk of major events like grounding and collision	Score 2 due to connection to business network for access internet	Risk = 4 x 2 = 8	Disconnect from business network	Risk = 4 x 1 = 4
4		EMAIL	Score 4 due to risk of major events like spamming/phising Email	Score 2 due to Security Email	Risk = 4 x 2 = 8	Have Security Email	Risk = 4 x 1 = 4
5	Bridge systems	ECDIS	Score 5 due to risk of catastrophic events like grounding and collision	Score 4 due to active USB ports, computer used for other purposes, connection to admin network for access to shared printer, connection to automatic chart updates via satellite via trusted vendor	Risk = 5 x 4 = 20	Password protect and restrict PC use to ECDIS only	Risk = 5 x 3 = 15
						Disconnect from admin network	Risk = 5 x 2 = 10
						Blind off USB ports	Risk = 5 x 1 = 5
6		Radar and Radio Communication	Score 3 due to risk of moderate events like data and spoofing	Score 4 due to GPS spoofing, Autonomus vessel, Insufficient data protection	Risk = 3 x 4 = 12	GPS spoofing	Risk = 3 x 3 = 9
						No Autonomus vessel	Risk = 3 x 2 = 6
						Data protection	Risk = 3 x 1 = 6
7		AIS	Score 2 due to risk of minor events like open system and encryption	Score 3 due to open system, lack of encryption algorithms	Risk = 2 x 3 = 6	System Close	Risk = 2 x 2 = 4
						New encryption algorithms	Risk = 2 x 1 = 4
8	Core Infrastructure systems	Business Network	Score 5 due to risk of major events like cyber attack	Score 4 due to no firewall, access internet, network segment, connection to OT network	Risk = 5 x 5 = 25	Add Firewall	Risk = 5 x 4 = 20
						Disconnect from admin network	Risk = 5 x 3 = 15
						Limit access internet	Risk = 5 x 2 = 10
						Different network	Risk = 5 x 1 = 5
9		OT Network	Score 3 due to risk of catastrophic events like cyber attack	Score 5 due to access internet, no firewall, network segment, connection to admin network	Risk = 5 x 5 = 75	Add Firewall	Risk = 5 x 4 = 20
						Disconnect from admin network	Risk = 5 x 3 = 15
						No access internet	Risk = 5 x 2 = 10
						Different network	Risk = 5 x 1 = 5
10	Passenger-facing networks	Passenger/Public	Score 4 due to risk of major events like cyber attack	Score 4 due to open access internet, no firewall, same segment IP with business network for shared folder or printer share	Risk = 4 x 4 = 16	Add Firewall	Risk = 4 x 3 = 12
						Limit access internet	Risk = 4 x 2 = 8
						Different network	Risk = 4 x 1 = 4
11	Administrative and crew welfare systems	Crew	Score 4 due to risk of major events like cyber attack	Score 4 due to active USB ports, no Firewall, connection to business network for access internet via satellite	Risk = 4 x 4 = 16	Add Firewall	Risk = 4 x 3 = 12
						Limit access internet	Risk = 4 x 2 = 8
						Blind off USB ports	Risk = 4 x 1 = 4

Sumber: data olahan

Gambar 28
Initial Risk Acceptance System

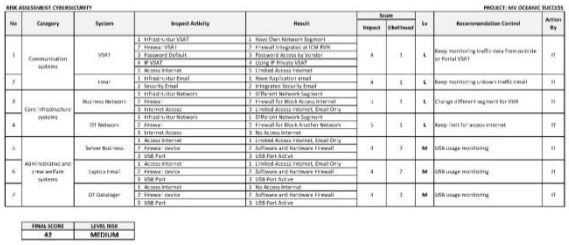
Hasil Risk Assessment

Setelah dilakukan tahap pengukuran selanjutnya melakukan perhitungan *final score assessment* Gambar 29 yang didapat dari akumulasi nilai *assessment*.

Final Risk Assessment - Unweighted & Averaged - Scoring Range (1 to 125)			
Low (1-27)	Medium (28-59)	High (60-99)	Extreme (100-125)

Sumber: data olahan

Gambar 29
Final Score Risk Assessment



RISK ASSESSMENT CYBERSECURITY — PROJECT: MV OCEANIC SUCCESS

No	Category	System	Inspect Activity	Result	Score: Impact	Score: Likelihood	Ex	Recommendation Control	Action By
1	Communication systems	VSAT	1. Infrastructur VSAT 2. Hirewa : VSAT 3. Password Default 4. IP VSAT 5. Access Internet	1. Have Own Network Segment 2. Firewall Integrated at ITM WSN 3. Password Access by Vendor 4. Using IP Private VSAT 5. Limited Access Internet	4	3	L	Keep monitoring traffic data from outside or Portal VSAT	IT
2		Email	1. Infrastructur Email 2. Security Email 3. Internet Access	1. Have Application email 2. Integrate Security Email 3. Limited Access Internet, Email Only	4	1	L	Keep monitoring unkown traffic Email	IT
3	Core Infrastructure systems	Business Network	1. Infrastructur Networks 2. Hirewa : 3. Internet Access	1. Different Network Segment 2. Firewall for Block Access Internet 3. Limited Access Internet, Email Only	3	1	L	Change different segment for VSAT	IT
4		OT Network	1. Infrastructur Networks 2. Hirewa : 3. Internet Access	1. Different Network Segment 2. Firewall for Block Another Network 3. No Access Internet	3	1	L	Keep Tetil for access internet	IT
5	Administrative and crew welfare systems	Server Business	1. Access Internet 2. Hirewa : Device 3. USB Port	1. Limited Access Internet, Email Only 2. Software and Hardware Firewall 3. USB Port Active	4	2	M	USB usage monitoring	IT
6		Laptop Email	1. Access Internet 2. Hirewa : Device 3. USB Port	1. Limited Access Internet, Email Only 2. Software and Hardware Firewall 3. USB Port Active	4	2	M	USB usage monitoring	IT
7		OT Datalogger	1. Access Internet 2. Hirewa : Device 3. USB Port	1. No Access Internet 2. Software and Hardware Firewall 3. USB Port Active	4	2	M	USB usage monitoring	IT

FINAL SCORE	LEVEL RISK
42	MEDIUM

Sumber: data olahan

Gambar 30
Hasil *Risk Assessment*

Hasil dari laporan cyber risk assessment Gambar 30, keamanan siber kapal milik PT Indobaruna Bulk Transport pada project MV. Oceanic Success, mendapatkan nilai scoring 42 (empat puluh dua) masuk ke dalam kategori level medium. Adapun rekomendasi kontrol keamanan yaitu pengawasan atau kebijakan dalam penggunaan perangkat usb flashdisk pada pemakaian komputer, hasil dari assessment ditemukan interface usb port dengan kondisi bisa digunakan.

SIMPULAN

Berdasarkan hasil dan pembahasan yang dilakukan dalam penelitian ini, peneliti menarik kesimpulan sebagai berikut struktur jaringan kapal terdiri dari dua bagian utama: operasional kerja dan operasional kapal, masing-masing dengan sistem *firewall* sendiri dan memiliki segmentasi alamat IP *address* yang berbeda-beda. Penggunaan *framework* NIST, CIA model dan *Risk Assessment Matrix* (RAM) untuk identifikasi dan pengukuran dalam proses penilaian keamanan siber pada sistem transportasi laut infrastruktur kapal. Serangan siber pada sistem transportasi laut infrastruktur kapal IBT, berdasarkan hasil *risk assessment report* masuk dalam kategori medium dengan hasil *scoring* 42 (empat puluh dua) *point*.

DAFTAR PUSTAKA

Amro, A., Oruc, A., Gkioulos, V., Katsikas, S. 2022. Navigation Data Anomaly Analysis and Detection. *Jurnal MDPI*

Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. 2022. Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. *Information (Switzerland)*, 13(1). MDPI.

BIMCO. 2021. *The Guidelines On Cyber Security Onboard Ships*. The Baltic and International Maritime Council.

Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. 2020. A novel cyber-risk assessment method for ship systems. *Safety Science*, 131.

Lee, Y.-C., Park, S.-K., Lee, W.-K., & Kang, J. 2017. Improving cyber security awareness in maritime transport : A way forward. *Journal of the Korean Society of Marine Engineering*, 41(8), 738–745

Pavur J., 2020, *Whispers Among the Stars*, Las Vegas, NV, Black Hat

US Coast Guard. 2019. *Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels*. Safety Alert 06-19. Homeland Security, Washington, DC.