**KEMENTERIAN PERHUBUNGAN**

**BADAN PENGEMBANGAN SDM PERHUBUNGAN**

**SEKOLAH TINGGI ILMU PELAYARAN**

# MAKALAH

# PENERAPAN MANAJEMEN RISIKO *CYBER SECURITY* DI ATAS MV. EVER OCEAN UNTUK MEWUJUDKAN KEAMANAN TEKNOLOGI INFORMASI DIERA *SOCIETY* 5.0


**Oleh :**

**OVER GRAND HUTAURUK**

**NIS. 02876/N-I**


**PROGRAM PENDIDIKAN DIKLAT PELAUT - 1**

**JAKARTA**

**2023**

**KEMENTERIAN PERHUBUNGAN**

**BADAN PENGEMBANGAN SDM PERHUBUNGAN**

**SEKOLAH TINGGI ILMU PELAYARAN**

# MAKALAH

# PENERAPAN MANAJEMEN RISIKO *CYBER SECURITY* DI ATAS MV. EVER OCEAN UNTUK MEWUJUDKAN KEAMANAN TEKNOLOGI INFORMASI DIERA *SOCIETY* 5.0

**Diajukan Guna Memenuhi Persyaratan**
**Untuk Menyelesaikan Program ANT - I**


**Oleh :**

**OVER GRAND HUTAURUK**

**NIS. 02876/N-I**


**PROGRAM PENDIDIKAN DIKLAT PELAUT - 1**

**JAKARTA**

**2023**

**KEMENTERIAN PERHUBUNGAN**

**BADAN PENGEMBANGAN SDM PERHUBUNGAN**

**SEKOLAH TINGGI ILMU PELAYARAN**

# TANDA PERSETUJUAN MAKALAH

| | | |
|---|---|---|
| Nama | : | OVER GRAND HUTAURUK |
| No. Induk Siswa | : | 02876/N-I |
| Program Pendidikan | : | DIKLAT PELAUT - I |
| Jurusan | : | NAUTIKA |
| Judul | : | PENERAPAN MANAJEMEN RISIKO *CYBER SECURITY* DI ATAS MV. EVER OCEAN UNTUK MEWUJUDKAN KEAMANAN TEKNOLOGI INFORMASI DIERA SOCIETY 5.0 |

Jakarta, 13 September 2023

| Pembimbing I, | Pembimbing II, |
|---|---|
| **Bhima Siswo Putro, S.Si.T., MM** | **Ronald Simanjuntak, M.T** |
| Penata TK.I ( III/c) | Pembina ( IV/a ) |
| NIP.19730526 200812 1 001 | NIP.19750616 200604 1 001 |

Mengetahui
Ketua Jurusan Nautika

**Meilinasari N. H., S.Si.T., M.M.Tr**
Penata Tk.I (III/d)
NIP. 19810503 200212 2 001

**KEMENTERIAN PERHUBUNGAN**

**BADAN PENGEMBANGAN SDM PERHUBUNGAN**

**SEKOLAH TINGGI ILMU PELAYARAN**

# TANDA PENGESAHAN MAKALAH

| | | |
|---|---|---|
| Nama | : | OVER GRAND HUTAURUK |
| No. Induk Siswa | : | 02876/N-I |
| Program Pendidikan | : | DIKLAT PELAUT - I |
| Jurusan | : | NAUTIKA |
| Judul | : | PENERAPAN MANAJEMEN RISIKO *CYBER SECURITY* DI ATAS MV. EVER OCEAN UNTUK MEWUJUDKAN KEAMANAN TEKNOLOGI INFORMASI DIERA SOCIETY 5.0 |

| Penguji I | Penguji II | Penguji III |
|---|---|---|
| **Capt. Fausil , MM** | **Roma Dormawaty, S.Si.T.,MM** | **Bhima Siswo Putro, S.Si.T.,MM** |
| Dosen STIP | Penata TK.I ( III/d ) | Penata TK.I ( III/c ) |
| | NIP.19790413 200212 2 001 | NIP.19730526 200812 1 001 |

Mengetahui
Ketua Jurusan Nautika

**Meilinasari N. H., S.Si.T., M.M.Tr**
Penata Tk.I (III/d)
NIP. 19810503 200212 2 001

# KATA PENGANTAR

Dengan memanjatkan puja dan puji syukur kehadirat Allah SWT. Karena atas berkat rahmat, taufik dan hidayah-Nya sehingga dapat menyelesaikan makalah ini tepat pada waktunya dan sesuai dengan yang diharapkan. Adapun penyusunan makalah ini guna memenuhi persyaratan penyelesaian Program Diklat Pelaut Ahli Nautika Tingkat I (ANT - l) pada Sekolah Tinggi Ilmu Pelayaran (STIP) Jakarta.

Pada penulisan makalah ini penulis tertarik untuk menyoroti atau membahas tentang keselamatan kerja dan mengambil judul :

**"PENERAPAN MANAJEMEN RISIKO *CYBER SECURITY* DI ATAS MV. EVER OCEAN UNTUK MEWUJUDKAN KEAMANAN TEKNOLOGI INFORMASI DIERA SOCIETY 5.0"**

Tujuan penulisan makalah ini adalah untuk memenuhi salah satu persyaratan yang wajib dilaksanakan oleh setiap perwira siswa dalam menyelesaikan pendidikan di Sekolah Tinggi Ilmu Pelayaran ( STIP ) Jakarta pada jenjang terakhir pendidikan. Sesuai Keputusan Kepala Badan Pendidikan dan Latihan Perhubungan Nomor 233/HK-602/Diklat-98 dan mengacu pada ketentuan Konvensi International STCW-78 Amandemen 2010

Makalah ini diselesaikan berdasarkan pengalaman bekerja penulis sebagai Perwira di atas kapal ditambah pengalaman lain yang penulis dapatkan dari buku-buku dan literatur. Penulis menyadari bahwa makalah ini jauh dari kesempurnaan Hal ini disebabkan oleh keterbatasan-keterbatasan yang ada Ilmu pengetahuan, data-data, buku-buku, materi serta tata bahasa yang penulis miliki.

Dalam kesempatan yang baik ini pula, penulis menyampaikan ucapan terima kasih yang tak terhingga disertai dengan doa kepada Allah Tuhan Yang Maha Kuasa untuk semua pihak yang turut membantu hingga terselesainya penulisan makalah ini, terutama kepada Yang Terhormat:

1. H. Ahmad Wahid, S.T., M.T., M.Mar.E, selaku Ketua Sekolah Tinggi Ilmu Pelayaran (STIP) Jakarta.
2. Ibu Meilinasari N. H,S.Si.T.,M.M.Tr, selaku Ketua Jurusan Nautika Sekolah Tinggi Ilmu Pelayaran Jakarta.

3. Capt. Suhartini, S.SiT.,M.M.,M.MTr, selaku Kepala Divisi Pengembangan Usaha Sekolah tinggi Ilmu Pelayaran (STIP) Jakarta.
4. Bhima Siswo Putro, S.SiT., MM, sebagai Dosen Pembimbing I atas seluruh waktu yang diluangkan untuk penulis serta materi, ide/gagasan dan moril hingga terselesaikan makalah ini.
5. Ronald Simanjuntak, M.T, sebagai Dosen Pembimbing II atas seluruh waktu yang diluangkan untuk penulis serta materi, ide/gagasan dan moril hingga terselesaikan makalah ini.
6. Para Dosen Pengajar STIP Jakarta yang secara langsung ataupun tidak langsung yang telah memberikan bantuan dan petunjuknya.
7. Orang Tua Tercinta yang membantu atas doa dan bantuan selama pembuatan makalah.
8. Istri Tercinta yang membantu atas doa dan bantuan selama pembuatan makalah.
9. Semua rekan-rekan Pasis Ahli Nautika Tingkat I Angkatan LXVII tahun ajaran 2023 yang telah memberikan bimbingan, sumbangsih dan saran baik secara materil maupun moril sehingga makalah ini akhirnya dapat terselesaikan.

Akhir kata penulis mengharapkan semoga makalah ini dapat bermanfaat bagi penulis sendiri maupun pihak-pihak yang membaca dan membutuhkan makalah ini terutama dari kalangan Akademis Sekolah Tinggi Ilmu Pelayaran (STIP) Jakarta.

Jakarta, 13 September 2023

Penulis,

OVER GRAND HUTAURUK

NIS. 02876/N-I

# DAFTAR ISI

**Halaman**

# DAFTAR TABEL

# DAFTAR GAMBAR

# DAFTAR LAMPIRAN

# BAB I
# PENDAHULUAN

## A. LATAR BELAKANG

Dalam era digital yang terus berkembang, teknologi informasi dan komunikasi memiliki peran yang krusial dalam kehidupan sehari-hari, bisnis, dan pemerintahan. Namun, seiring dengan kemajuan teknologi, risiko keamanan *cyber* juga semakin meningkat. Ancaman-ancaman seperti serangan *cyber*, peretasan data, pencurian identitas, *malware*, dan kejahatan *cyber* lainnya telah menjadi ancaman yang serius bagi organisasi dan individu di seluruh dunia. Keamanan Teknologi Informasi dalam era *Society* 5.0 merujuk pada upaya perlindungan dan pengamanan sistem informasi, data, serta infrastruktur teknologi dalam konteks masyarakat yang semakin terhubung dan tergantung pada teknologi digital. *Society* 5.0 merupakan konsep perkembangan masyarakat yang menggabungkan dunia fisik (*analog*) dengan dunia digital (*digital*) melalui penggunaan teknologi *seperti internet of things* (IoT), *big data*, robotika, dan lain-lain.

. Manajemen risiko *cyber security* merupakan proses yang melibatkan identifikasi, analisis, dan pengelolaan risiko yang terkait dengan ancaman keamanan *cyber*. Tujuan utama dari manajemen risiko *cyber security* adalah untuk mengurangi risiko yang ditimbulkan oleh serangan *cyber* dan menjaga keberlanjutan operasional serta keamanan sistem dan data. Dalam konteks ini, organisasi dan entitas lainnya secara sistematis menganalisis potensi kerentanan dalam infrastruktur teknologi informasi, mengukur dampak dari ancaman yang mungkin terjadi, dan mengembangkan langkah-langkah pencegahan serta rencana tanggap darurat yang sesuai. Manajemen risiko *cyber security* melibatkan koordinasi lintas-fungsional, termasuk aspek teknis, kebijakan, pelatihan, dan komunikasi, guna menciptakan lingkungan yang aman, melindungi data sensitif, dan memastikan kelangsungan operasional. Dengan mengadopsi pendekatan ini, organisasi dapat memitigasi risiko yang terkait dengan serangan *cyber*, pencurian

data, dan kerentanan teknologi, serta merespons dengan cepat dalam menghadapi insiden keamanan *cyber* agar dampak negatif dapat diminimalkan.

Penerapan *cyber security* di atas kapal merupakan hal yang sangat penting mengingat kapal modern sangat bergantung pada sistem teknologi informasi dan komunikasi untuk berbagai aspek operasional. Kapal modern dilengkapi dengan berbagai sistem otomatisasi, sensor, dan perangkat elektronik yang menghubungkan kapal dengan dunia luar melalui jaringan komunikasi. Namun, ini juga membuka celah bagi serangan *cyber* yang dapat mengganggu operasional kapal, mengancam keselamatan *crew*, dan menyebabkan kerugian finansial yang signifikan.

Dalam penerapan manajemen risiko *cyber security* di atas kapal, aspek teknis sangat penting. Ini melibatkan penggunaan teknologi keamanan yang tepat untuk melindungi sistem dan data. Misalnya, *download* dan *update virus*, penerapan *firewall*, sistem deteksi intrusi, enkripsi data, dan pembaruan keamanan terkini pada perangkat keras dan perangkat lunak. Selain itu, juga perlu dilakukan pemantauan secara aktif terhadap jaringan untuk mendeteksi adanya serangan atau aktivitas mencurigakan.

Manajemen risiko *cyber security* di atas kapal membutuhkan kebijakan yang jelas dan terdefinisi dengan baik. Kebijakan ini harus mencakup pedoman penggunaan sistem, pengelolaan kata sandi, akses yang diberikan kepada individu, serta tindakan yang harus diambil dalam menghadapi serangan *cyber*. Kebijakan ini juga harus diperbarui secara berkala sesuai dengan perkembangan teknologi dan ancaman keamanan yang terbaru.

Melibatkan *crew* dalam penerapan manajemen risiko *cyber security* sangat penting seperti pelatihan yang memadai tentang ancaman keamanan *cyber* dan tindakan pencegahan yang harus diambil. Pelatihan ini harus mencakup pemahaman tentang penggunaan yang aman dari sistem, identifikasi serangan *cyber*, dan tindakan yang harus diambil jika terjadi serangan. Manajemen risiko *cyber security* di atas kapal juga memerlukan komunikasi yang efektif antara semua pihak terkait. Ini termasuk koordinasi dengan pihak eksternal yang menyediakan layanan dan sistem yang terhubung dengan kapal. Komunikasi yang baik memastikan bahwa semua pihak memahami kebijakan keamanan yang ada,

melaporkan adanya kejadian mencurigakan, dan bekerja sama dalam menghadapi serangan *cyber*.

Berdasarkan pengalaman Penulis saat menjabat sebagai Mualim 2 di atas MV. EVER OCEAN, terdapat sebuah peristiwa pada tanggal 5 Juni 2023 pukul 10.00 *local time*, kapal menghadapi masalah serius akibat kurangnya pemahaman *crew* terhadap *cyber security*. Seorang *crew* yang tidak sengaja mengklik tautan yang mencurigakan dalam sebuah *email* yang ia terima di komputer yang berada di anjungan. Tanpa menyadari bahwa itu adalah serangan *phishing*, *malware* berhasil masuk ke sistem kapal. yang tersebar saat ini melalui perangkat USB. *Malware* yang telah ditemukan adalah *trickbot*, sebuah *trojan* yang menjadi ancaman. *Trojan* ini dirancang dengan tujuan membocorkan informasi *login* dari pengguna yang terinfeksi. *TrickBot* menyebar melalui email *phishing* yang mengandung lampiran berbahaya dan tautan yang mengarah ke situs *web* palsu.

Kemudian salah satu komputer terdeteksi terkena virus oleh *shore monitoring program* karena kru kapal menghubungkan laptop pribadi yang terinfeksi virus ke jaringan kapal, menyebabkan PC (*Personal Computer*) di dek kapal dan dua komputer umum yang tidak memperbarui *anti- virus definition* terinfeksi virus. Setelah dianalisis, virus tersebut diidentifikasi sebagai *cryptocurrency miner* untuk menyalin *malware* ke setiap *disk slot* dan menyebarluaskan melalui folder berbagi untuk terus menginfeksi lebih banyak komputer dan menyebarkan lebih banyak *cryptocurrency miner* setelah mendapatkan kesempatan untuk terhubung ke internet. Dampak dari *virus* yang dirancang dengan cermat untuk mengeksploitasi kelemahan sistem kapal menyebabkan masalah sistem yang serius pada komputer yang digunakan untuk memantau pengoperasian *main/auxiliary engines* dalam ruang mesin, sistem pemantauan *container*, *ballast water management system*, dan peralatan navigasi di anjungan yang mengakibatkan terganggunya aliran data, sehingga menyebabkan ketidakakuratan dalam memantau dan menganalisis.

Setelah insiden tersebut terjadi, dilakukan investigasi internal yang mengungkapkan bahwa kurangnya pemahaman *crew* terhadap *cyber security* menjadi penyebab utama kebocoran data dan *virus*. Mereka kurang dilatih dengan baik tentang ancaman keamanan *cyber* dan tindakan pencegahannya. Selain itu, kebijakan keamanan *cyber* yang jelas dan diterapkan dengan ketat masih kurang di atas kapal. Penting bagi kapal dan kru untuk mengambil tindakan pencegahan yang

serius dalam menghadapi ancaman keamanan *cyber*. Pendidikan, pelatihan, dan implementasi protokol keamanan yang kuat sangatlah penting untuk melindungi integritas dan keberlangsungan operasional kapal di dunia yang semakin terhubung secara digital.

Oleh karena itu, Penulis tertarik untuk mengulas permasalahan yang terjadi di atas kapal dalam makalah yang berjudul **"PENERAPAN MANAJEMEN RISIKO *CYBER SECURITY* DI ATAS MV. EVER OCEAN UNTUK MEWUJUDKAN KEAMANAN TEKNOLOGI INFORMASI DIERA SOCIETY 5.0".**

## B. IDENTIFIKASI, BATASAN DAN RUMUSAN MASALAH

### 1. Identifikasi Masalah

Dalam penulisan makalah Penulis mengidentifikasikan beberapa masalah yang terjadi di MV. EVER OCEAN sebagai berikut:

a. Kurangnya pemahaman *crew* terhadap *cyber security* diatas kapal berdampak bocornya data-data perusahaan.
b. Terjadinya serangan virus tertentu yang mengancam keamanan sistem komputer kapal.
c. Turunnya kinerja komputerisasi yang ada diatas kapal.
d. Kurangnya pelatihan mendalam *crew* tentang *cyber security*.
e. Kurangnya pengetahuan *crew* tentang serangan *cyber.*

### 2. Batasan Masalah

Agar pembahasan tidak meluas, maka Penulis akan membatasi masalah hanya pada:

a. Kurangnya pemahaman *crew* terhadap *cyber security* diatas kapal berdampak bocornya data-data perusahaan.
b. Terjadinya serangan *virus* tertentu yang mengancam keamanan sistem komputer kapal.

### 3. Rumusan Masalah

Berdasarkan permasalahan pada latar belakang, maka rumusan masalah dalam penelitian ini adalah:

a. Apa penyebab kurangnya pemahaman *crew* terhadap *cyber security* diatas kapal berdampak bocornya data-data perusahaan?

b. Bagaimana serangan *virus* tertentu yang mengancam keamanan sistem komputer kapal?

## C. TUJUAN DAN MANFAAT PENELITIAN

### 1. Tujuan Penelitian

Tujuan dari penelitian yang dilakukan oleh Penulis adalah:

a. Untuk mengidentifikasi dan menganalisis faktor-faktor yang berkontribusi terhadap kurangnya pemahaman awak kapal tentang *cyber security*?.

b. Untuk menganalisis masalah yang muncul akibat serangan virus tertentu yang mengancam keamanan sistem komputer kapal.

### 2. Manfaat Penelitian

Beberapa manfaat yang diharapkan dari hasil penelitian ini adalah :

#### a. Aspek Teoritis

1) Penelitian ini dapat mengidentifikasi dan menganalisis faktor-faktor yang berkontribusi terhadap kurangnya pemahaman awak kapal tentang *cyber security*.

2) Penelitian ini dapat memberikan wawasan yang berharga dalam pengembangan pedoman dan kebijakan mencegah serangan *virus* yang mengancam sistem komputer kapal.

#### b. Aspek Praktis

1) Diharapkan Penelitian ini dapat memberikan panduan yang lebih efektif dalam merancang dan mengimplementasikan program pelatihan *cyber security* untuk awak kapal.

2) Diharapkan penelitian ini dapat memberikan panduan dan rekomendasi praktis untuk meningkatkan perlindungan data perusahaan di kapal.

3) Sebagai syarat untuk memperoleh gelar *Master Marine* di STIP Jakarta.

## D. METODE PENELITIAN

### 1. Jenis Penelitian

Penulis menggunakan jenis penelitian kualitatif dalam penelitian ini. Penelitian kualitatif adalah prosedur penelitian yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari orang-orang yang dapat diamati, yang diperoleh langsung dari tempat kejadian. Selain itu, penelitian ini juga menggunakan sumber data berupa berita-berita dan buku-buku yang relevan dengan permasalahan yang diteliti. Dalam penelitian ini, Penulis menggunakan pendekatan kualitatif untuk memperoleh pemahaman yang mendalam tentang kurangnya pemahaman *crew* terhadap *cyber security* diatas kapal berdampak bocornya data-data perusahaan dan terjadinya serangan *virus* yang mengancam sistem komputer kapal. Dengan menggunakan jenis penelitian kualitatif, Penulis dapat mengumpulkan data yang kaya akan informasi dan memperoleh wawasan yang lebih mendalam tentang faktor-faktor yang mempengaruhi permasalahan tersebut.

Penelitian merupakan suatu proses yang dilakukan secara terencana dan sistematis untuk mendapatkan pemecahan masalah atau jawaban terhadap pernyataan-pernyataan tertentu. Melalui penelitian, para peneliti mengikuti langkah-langkah yang telah dirancang dengan baik untuk mengumpulkan, menganalisis, dan menginterpretasi data. Tujuan utama dari penelitian adalah untuk mendapatkan pemahaman yang lebih mendalam tentang suatu fenomena atau untuk menghasilkan pengetahuan baru yang dapat digunakan untuk memecahkan masalah atau menjawab pertanyaan-pertanyaan yang ada.

Menurut M.A. Ibrahim (2015: 55) dalam bukunya yang berjudul "Metodologi Penelitian Kualitatif", Pendekatan Kualitatif adalah cara kerja penelitian yang menekankan pada aspek pendalaman data demi mendapatkan kualitas dari hasil suatu penelitian. Dengan kata lain, pendekatan kualitatif (*qualitative approach*) adalah suatu mekanisme kerja penelitian yang mengandalkan uraian deskriptif kata, atau kalimat, yang disusun secara cermat dan sistematis mulai dari menghimpun data hingga menafsirkan dan melaporkan hasil penelitian.

Penelitian merupakan refleksi keinginan untuk memperoleh dan mengembangkan pengetahuan. Manusia secara alami memiliki keinginan untuk memahami dunia di sekitarnya dan menjawab pertanyaan-pertanyaan yang ada. Inilah yang menjadi motivasi untuk melakukan penelitian. Jenis metode yang digunakan dalam penelitian ini adalah dengan menggunakan metode deskriptif.

Metode deskriptif adalah salah satu cara kerja penelitian yang bertujuan untuk menggambarkan atau melukiskan keadaan suatu objek atau fenomena dengan seakurat mungkin. Metode ini dilakukan dengan memaparkan situasi dan kondisi yang ada pada saat penelitian dilakukan.

**2. Sumber Data**

Data adalah segala bentuk informasi, fakta dan realita yang terkait atau relevan dengan apa yang dikaji atau diteliti. Data dalam konteks ini bisa berupa kata-kata, lambang, simbol, ataupun situasi dan kondisi nyata yang terkait dengan penelitian yang dilakukan. Sedangkan sumber data dalam penelitian adalah orang, benda, objek yang dapat memberikan informasi, fakta, data, dan realitas yang terkait atau relevan dengan apa yang dikaji atau diteliti (M.A. Ibrahim, 2015: 67).

Data yang dikumpulkan dan digunakan dalam penyusunan makalah ini adalah data yang merupakan informasi yang diperoleh Penulis melalui pengamatan langsung dan wawancara. Dari sumber-sumber ini diperoleh data sebagai berikut :

**a. Data Primer**

Data primer adalah segala informasi, fakta, dan realitas yang terkait atau relevan dengan penelitian, dimana kaitan atau relevansikan sangat jelas, bahkan secara langsung. Disebut sebagai data utama (*primer*), karena data tersebut menjadi penentu utama berhasil atau tidaknya sebuah penelitian. Artinya, hanya dengan didapatkannya data tersebut sebuah penelitian dapat dikatakan berhasil dikerjakan. Dari data itulah pertanyaan utama penelitian dapat dijawab. Dan dari data itu pula, penelitian tersebut dapat dikembangkan menjadi lebih detil, mendalam dan rinci. Data yang memiliki karakteristik seperti inilah yang disebut dengan data utama atau *primer* (M.A. Ibrahim, 2015: 68). Data ini diperoleh dari pengamatan langsung

dengan metode survei yaitu dengan cara mengamati dan mencatat secara langsung di tempat penelitian.

1) Teknik Observasi (Pengamatan)

Menurut Widoyoko (2014 :46) observasi merupakan pengamatan dan pencatatan secara sistematis terhadap unsur-unsur yang nampak dalam suatu gejala pada objek penelitian. Dalam observasi, peneliti secara teliti mengamati dan mencatat semua hal yang terlihat dan relevan dengan tujuan penelitian. Observasi dilakukan dengan tujuan untuk mengumpulkan data yang akurat dan mendapatkan pemahaman yang lebih baik tentang objek penelitian.

Observasi dilakukan dengan mengamati interaksi awak kapal dengan sistem komputer, kebijakan yang ada, dan kesadaran *crew* tentang ancaman keamanan *cyber*. Observasi mencakup pengamatan langsung terhadap tindakan awak kapal, penggunaan perangkat lunak keamanan, atau penerapan prosedur keamanan.

Melalui observasi, Penulis mengumpulkan data tentang tingkat pemahaman awak kapal terhadap *cyber security*, kelemahan dalam implementasi kebijakan dan prosedur keamanan, serta faktor-faktor lain yang berkontribusi terhadap kurangnya pemahaman tersebut. Observasi membantu dalam mengidentifikasi situasi atau perilaku yang berpotensi menyebabkan bocornya data perusahaan dan serangan *virus* di kapal.

2) Teknik Wawancara (*Interview*)

Menurut Kriyantono (2020: 289) wawancara dalam riset kualitatif, dapat juga disebut sebagai wawancara mendalam (*depth interview*) atau wawancara intesif (*intensive interview*) dan kebanyakan tidak berstruktur. Wawancara dalam riset kualitatif dilakukan dengan tujuan untuk mendapatkan data kualitatif yang mendalam.

Wawancara merupakan suatu metode yang digunakan dalam suatu penelitian untuk mendapatkan data dan informasi dengan cara tanya jawab atau dialog dengan narasumber yang bersangkutan. Wawancara memungkinkan Penulis untuk mendapatkan informasi yang lebih kualitatif dan mendalam mengenai persepsi, sikap, dan pengetahuan

awak kapal terkait *cyber security*. Selain itu, wawancara membantu dalam mengidentifikasi potensi solusi atau tindakan yang dapat diambil untuk meningkatkan pemahaman awak kapal dan mencegah bocornya data serta serangan virus di kapal.

**b. Data Sekunder**

Data sekunder adalah segala informasi, fakta dan realitas yang juga terkait atau relevan dengan penelitian, namun tidak secara langsung, atau tidak begitu jelas relevansi. Bahkan data sekunder ini lebih bersifat kulitnya saja, yang tidak mampu menggambarkan substansi terdalam dari informasi, fakta dan realitas yang dikaji atau diteliti. Sebagai data pendukung (sekunder), informasi ini memang tidak menentukan (tidak substantif), akan tetapi data ini bisa memperjelas gambaran sebuah realitas penelitian (M.A. Ibrahim, 2015: 68). Data ini merupakan data pelengkap yang diperoleh dari literatur/gambar, yang berhubungan dengan penelitian ini. Data Sekunder diperoleh dengan teknik dokumentasi. Dokumentasi adalah pengumpulan, pemilihan, pengolahan, dan penyimpanan informasi di bidang pengetahuan, artinya dokumentasi adalah mengumpulkan data dan memilah-milah berdasarkan kebutuhan penelitian kemudian mengolahnya menjadi sebuah informasi. Dokumentasi yang ditunjukkan dalam hal ini adalah segala dokumen yang berhubungan dengan kelembagaan dan administrasi, struktur manajemen. Dalam konteks ini, Penulis akan menggunakan beberapa data sekunder yang antara lain berasal dari perusahaan, seperti *Ship Particular* dan *Crew List*. Data tersebut akan dijadikan referensi dalam penelitian yang sedang dilakukan oleh Penulis.

*Ship Particular* adalah sebuah dataset yang memberikan informasi terperinci mengenai karakteristik dan spesifikasi teknis suatu kapal. Data ini mencakup berbagai informasi seperti nama kapal, jenis kapal, ukuran, bobot mati (DWT), negara bendera, serta informasi lain yang relevan seperti spesifikasi mesin, sistem navigasi, dan peralatan kapal lainnya. Dengan menggunakan *Ship Particular*, dapat memperoleh pemahaman yang mendalam tentang kapal tersebut dan dapat menganalisis kemampuan serta fitur teknis yang dimilikinya.

*Crew List* adalah daftar lengkap dari awak kapal yang berisi informasi tentang nama, jabatan, dan tugas masing-masing anggota awak kapal. Data ini memberikan gambaran yang komprehensif tentang personel yang terlibat dalam operasi dan pengoperasian kapal. Dengan memahami struktur dan peran awak kapal melalui *Crew List*, dapat memperoleh pemahaman yang lebih baik tentang bagaimana awak kapal berkontribusi dalam menjalankan kapal secara efektif dan efisien.

Berdasarkan latar belakang dan perumusan masalah tersebut di atas, maka dalam penyusunan makalah ini membutuhkan suatu pengamatan agar mampu mendapatkan data yang benar, sehingga tujuan penulisan dapat tercapai dan sesuai dengan judul yang telah diterapkan.

**3. Pemilihan informan**

Pada penelitian ini, informan penelitian merupakan awak kapal MV. EVER OCEAN yang meliputi berbagai peran di kapal, seperti kapten, perwira keamanan, teknisi IT, atau anggota kru lainnya yang terlibat dalam pengoperasian dan pemeliharaan sistem komputer di kapal yang memiliki wawasan langsung tentang kurangnya pemahaman awak kapal terhadap *cyber security* di atas kapal, serta dampak bocornya data perusahaan dan serangan virus tertentu yang dapat mengancam keamanan sistem komputer kapal.

**4. Teknik Analisa Data**

Penyajian untuk penulisan makalah ini adalah menggunakan metode deskriptif. Yaitu penulisan yang berisi paparan dan uraian mengenai suatu objek permasalahan yang timbul pada saat tertentu. Metode ini digunakan untuk memaparkan secara rinci dengan tujuan memberikan informasi mengenai masalah yang timbul dan berhubungan dengan materi pembahasan makalah.

Menurut Miles dan Huberman (dalam Sugiyono, 2019: 321) menyatakan bahwa aktivitas dalam pengolahan dan analisis data meliputi data *collecting, data reduction, data display, conclusion drawing/verification.* Langkag-langkah tersebut dapat dijelaskan sebagai berikut :

**a. Data *Collecting***

Instrumen pengumpulan data adalah alat bantu yang dipilih dan digunakan oleh peneliti dalam kegiatannya mengumpulkan data agar kegiatan tersebut menjadi sitematis dan dipermudah olehnya. Instrumen pengumpulan data adalah cara-cara yang dapat digunakan oleh peneliti untuk mengumpulkan data. Instrumen sebagai alat bantu dalam menggunakan metode pengumpulan data merupakan sarana yang dapat diwujudkan dalam benda, misalnya pedoman observasi dan sebagainya.

Instrumen penelitian merupakan sesuatu yang amat penting dan strategis kedudukannya di dalam keseluruhan kegiatan penelitian. Dengan instrumen akan diperoleh data yang merupakan bahan penting untuk menjawab pemersalahan, mencari sesuatu yang akan digunakan untuk mencapai tujuan. Pengumpulan data dilakukan untuk memperoleh informasi yang dibutuhkan dalam rangka mencapai tujuan penelitian.

**b. Data *Reduction***

Reduksi data merupakan proses pemilihan, pemusatan perhatian pada penyederhanaan, pengabstrakkan dan transformasi data yang muncul dari catatan-catatan tertulis dilapangan sebagaimana kita ketahui, reduksi data berlangsung terus-menerus selama proyek yang berorientasi kualitatif berlangsung. Reduksi data merupakan suatu bentuk analisis yang menajamkan, menggolongkan, mengarahkan, membuang yang tidak perlu dan mengorganisasi data dengan cara sedemikian rupa sehingga kesimpulan finalnya dapat ditarik dan diverifikasi.

**c. Data *Display***

Penyajian data dalam penelitian kualitatif adalah dengan teks yang bersifat deskriptif. Dengan menggunakan informasi yang diperoleh dari lapangan yang dituangkan berbentuk teks dengan sebaik mungkin tanpa adanya rekayasa dan penambahan yang tidak sesuai dengan penelitian. Hal tersebut dilakukan bertujuan agar penyajian data yang telah direduksi sesuai dengan keadaan yang sebenarnya. Dalam penelitian ini peneliti telah berusaha menyajikan data yang tepat dan akurat sesuai dengan permasalahan dan keadaan yang terdapat pada objek penelitian.

Pada tahap ini, penulis akan menyajikan data hasil dari langkah reduksi data, Adapun data yang akan penulis sajikan berupa deskriptif naratif dan gambar-gambar yang berkaitan dengan permasalahan yang akan di analisis.

**d. *Conclusion and Verification***

Setelah semua data yang berhubungan dengan permasalahan penelitian diperoleh serta menghubungkan dengan teori yang sesuai dengan permasalahan pada penelitian. Maka barulah didapatkan kesimpulan yang sempurna yang sesuai dengan jenis dan permasalahan penelitian. Dari beberapa data yang diperoleh kemudian dikembangkan dengan kerangka pemikiran dan teori yang telah didapat agar kesimpulan akhir sesuai dengan tujuan penelitian dan tidak menyimpang dari permasalahan.

## E. WAKTU DAN TEMPAT PENELITIAN

Penelitian ini dilakukan ketika Penulis bekerja sebagai Mualim 2 di MV. EVER OCEAN mulai dari tanggal 12 Februari 2022 hingga 25 Agustus 2023. Tempat penelitian berada di kapal tersebut. Dalam periode tersebut, Penulis memiliki kesempatan unik untuk melakukan penelitian tentang masalah yang berkaitan dengan *cyber security* diatas kapal secara langsung dari posisi Penulis sebagai Mualim 2. Pengalaman kerja Penulis di atas kapal memberikan wawasan yang berharga dan pemahaman mendalam tentang permasalahan yang terjadi dalam konteks *cyber security* tersebut. Dengan demikian, penelitian ini didasarkan pada pengalaman praktis yang Penulis peroleh selama periode tersebut.

## F. SISTEMATIKA PENULISAN

Untuk dapat memahami dan mendapatkan pandangan yang lebih jelas memenuhi pokok permasalahan yang dihadapi dan dibahas, diperlukan adanya sistematika penulisan dalam penyusunan penelitian ini. Sistematika penulisan dapat dijabarkan sebagai berikut :

**BAB I PENDAHULUAN**

Dalam bab ini di uraikan tentang latar belakang masalah, identifikasi batasan dan rumusan masalah, tujuan dan manfaat penelitian, metode penelitian, waktu dan tempat penelitian serta sistematika penulisan.

**BAB II LANDASAN TEORI**

Pada bab ini dijelaskan tentang teori-teori yang digunakan untuk menganalisa data-data yang didapat melalui buku-buku sebagai referensi untuk mendapatkan informasi dan juga sebagai tinjauan Pustaka. Pada landasan teori ini juga terdapat kerangka pemikiran yang merupakan model konseptual tentang bagaimana teori berhubungan dengan berbagai faktor yang telah diidentifikasi sebagai masalah yang penting.

**BAB III ANALISIS DAN PEMBAHASAN**

Bab ini berisikan data-data yang diambil dari lapangan sesuai dengan pengalaman Penulis selama bekerja di atas MV. EVER OCEAN. Data-data dirumuskan dalam sekripsi data, kemudian dianalisis permasalahan yang terjadi dan menjabarkan pemecahan dari permasalahan tersebut. Dengan demikian permasalahan yang sama tidak terjadi lagi. Dengan kata lain menawarkan solusi terhadap penyelesaian masalah tersebut.

**BAB IV KESIMPULAN DAN SARAN**

Pada bab ini dijelaskan tentang penutup yang mengemukan kesimpulan dari perumusan masalah yang dibahas dan saran yang berasal dari evaluasi pemecahan masalah yang dibahas di dalam penulisan makalah ini dan merupakan masukan untuk perbaikan yang akan dicapai.

**DAFTAR PUSTAKA**

**LAMPIRAN**

**PENJELASAN ISTILAH**

# BAB II
# LANDASAN TEORI

## A. TINJUAN PUSTAKA

Tinjauan pustaka adalah langkah penting dalam penelitian yang melibatkan pengumpulan, evaluasi, dan rangkuman teori-teori, penelitian terkait, dan informasi terbaru yang relevan dengan topik yang diteliti. Dalam konteks kurangnya pemahaman *crew* terhadap *cyber security* dan terjadinya serangan virus tertentu pada sistem kapal, tinjauan pustaka akan memberikan dasar teoritis yang kuat untuk mengidentifikasi masalah, merumuskan pertanyaan penelitian, dan mengembangkan solusi yang sesuai. Hal ini bertujuan untuk memberikan gambaran yang lebih jelas dan terinci mengenai tujuan dari penulisan ini dan hasil yang diharapkan dapat dicapai.

### 1. Pengertian Penerapan

Menurut Elok Nuriyanto (2020: 105), penerapan adalah sebuah tindakan yang dilakukan, baik secara individu maupun kelompok dengan maksud untuk mencapai tujuan yang telah dirumuskan. Proses ini terkait erat dengan tujuan organisasi, di mana tindakan yang dilakukan harus sesuai dengan rencana dan strategi yang telah dirumuskan. Dengan penerapan yang efektif, organisasi dapat mengimplementasikan kebijakan, mengadopsi perubahan, mengoptimalkan sumber daya, dan mencapai hasil yang diharapkan.

### 2. Teori Manajemen Teknologi Informasi

Menurut Eko Budi (2021: 227), ada 4 (empat) pondasi utama yang mendukung perkembangan teknologi informasi yaitu: perkembangan perangkat lunak (*software*) seperti sistem dan aplikasi dan perkembangan alat keras (*hardware*) perkembangan sarana dan prasarana teknologi informasi, manajemen isi (*content management*), *telecommunication and*

*networking*, perkembangan internet serta perdagangan *online* atau melalui internet. Sementara untuk pengorganisasian terkait dengan pengunaan sistem teknologi informasi setidaknya ada empat hal utama yang harus diperhatikan yaitu:

**a. Sistem informasi (*information systems*).**

Sistem informasi merupakan komponen penting dalam pengorganisasian karena berperan dalam mengumpulkan, mengelola, menyimpan, dan menyebarkan informasi yang relevan bagi suatu organisasi. Sistem informasi membantu mengintegrasikan berbagai proses dan fungsi organisasi, memfasilitasi aliran informasi antar departemen, mempercepat pengambilan keputusan, serta meningkatkan efisiensi dan efektivitas operasional. Dengan adanya sistem informasi yang baik, organisasi dapat mengoptimalkan penggunaan sumber daya, meningkatkan koordinasi dan kolaborasi antar anggota tim, serta merespons perubahan lingkungan dengan cepat dan tepat.

**b. Kompetisi Organisasi (*Organizational Competition*).**

Kompetisi organisasi merupakan dinamika yang terjadi antara organisasi-organisasi dalam upaya untuk mencapai keunggulan kompetitif di pasar. Dalam konteks pengorganisasian, kompetisi organisasi mendorong perusahaan untuk mengoptimalkan sumber daya, merancang struktur organisasi yang efisien, dan mengembangkan strategi yang inovatif untuk memenangkan persaingan. Kompetisi ini mempengaruhi pengambilan keputusan, pengaturan tujuan, dan pengorganisasian proses bisnis agar organisasi dapat beradaptasi dengan cepat, menghadapi tantangan pasar, dan menciptakan nilai yang superior bagi pelanggan.

**c. *Information Systems* dan *Organizational Decision Making* (Sistem Informasi dan Pengambilan Keputusan dalam Organisasi).**

Sistem informasi dan pengambilan keputusan dalam organisasi memiliki hubungan yang erat dengan pengorganisasian. Sistem informasi adalah kerangka kerja yang mengintegrasikan teknologi informasi, proses bisnis, dan sumber daya manusia untuk mengumpulkan, mengelola,

menyimpan, dan menyebarkan informasi yang relevan bagi organisasi. Sistem informasi ini memainkan peran penting dalam pengorganisasian, karena memberikan akses terhadap informasi yang diperlukan untuk pengambilan keputusan yang efektif. Pengambilan keputusan, di sisi lain, merupakan proses penting dalam pengorganisasian yang melibatkan analisis informasi, pemilihan alternatif, dan penentuan tindakan yang tepat. Dengan adanya sistem informasi yang baik, organisasi dapat mengumpulkan data yang relevan, menganalisisnya, dan mengambil keputusan yang lebih baik, yang pada gilirannya mendukung pengorganisasian yang efisien dan efektif.

**d. Pengorganisasian Penggunaan System Informasi (*Organizational Use of Information Systems*).**

Pengorganisasian penggunaan sistem informasi dalam kaitannya dengan pengorganisasian adalah proses mengatur dan mengelola sistem informasi di dalam organisasi untuk mencapai tujuan dan kebutuhan bisnis. Dalam pengorganisasian, sistem informasi digunakan untuk mengintegrasikan berbagai fungsi dan departemen dalam organisasi, memfasilitasi aliran informasi yang lancar, dan meningkatkan efisiensi operasional. Dengan penggunaan yang tepat, sistem informasi dapat mempercepat pengambilan keputusan, memperbaiki kolaborasi antar tim, dan meningkatkan produktivitas keseluruhan organisasi. Selain itu, sistem informasi juga dapat membantu dalam pengorganisasian sumber daya, seperti pengelolaan inventaris, pengelolaan rantai pasok, dan pemantauan kinerja. Dengan demikian, pengorganisasian penggunaan sistem informasi merupakan faktor penting dalam menjaga keberhasilan dan daya saing organisasi di era digital saat ini.

**3. *Cyber-Risk Management***

Menurut Obrina Candra Briliyant (2020: 2), c*yber-risk management* dapat diartikan sebagai langkah pengelolaan berkelanjutan dalam menghadapi risiko *cyber* dan ketidakpastian agar mampu memaksimalkan pencapaian tujuan organisasi.

Risiko *cyber* merupakan risiko yang disebabkan oleh adanya ancaman *cyber* di dalam ruang *cyber* siber. Ruang *cyber* merupakan sekumpulan komputer yang terhubung dalam satu jaringan termasuk layanan, sistem komputer, *embedded processor, controller*, hingga informasi yang disimpan atau ditransmisikan melaluinya. Pada umumnya, ancaman *cyber* ditujukan terhadap *cyber-system*. *Cyber-system* merupakan suatu sistem yang dibuat dan penggunaannya bergantung pada ruang *cyber*. Adanya *cyber-system* tersebut menuntut organisasi untuk menyadari kerawanan sistemnya terhadap ancaman *cyber*.

Penerapan manajemen risiko *cyber security* melibatkan serangkaian langkah dan tindakan untuk menjaga keamanan teknologi informasi. Berikut adalah beberapa aspek yang perlu dipertimbangkan dalam penerapan manajemen risiko *cyber security*:

**a. Identifikasi Risiko**

Langkah pertama adalah mengidentifikasi berbagai risiko *cyber security* yang mungkin dihadapi oleh kapal dan sistem teknologi informasinya. Ini melibatkan penilaian terhadap ancaman yang mungkin, seperti serangan siber, pencurian data, atau pelanggaran privasi. Identifikasi risiko ini harus mencakup seluruh aspek kapal, termasuk sistem komunikasi, sistem navigasi, dan sistem kontrol operasional.

**b. Evaluasi Risiko**

Setelah risiko diidentifikasi, langkah berikutnya adalah mengevaluasi tingkat risiko masing-masing dan dampaknya terhadap keamanan teknologi informasi dan operasional kapal. Evaluasi risiko ini dapat dilakukan dengan menganalisis kemungkinan terjadinya serangan serta potensi kerugian yang dapat ditimbulkan. Hal ini membantu dalam penetapan prioritas tindakan mitigasi dan alokasi sumber daya yang tepat.

**c. Mitigasi Risiko**

Setelah risiko dievaluasi, langkah selanjutnya adalah mengimplementasikan tindakan mitigasi untuk mengurangi atau menghilangkan risiko tersebut. Ini melibatkan penerapan kebijakan keamanan yang ketat, seperti penggunaan kata sandi yang kuat, akses

terbatas terhadap sistem, dan enkripsi data. Selain itu, dapat dilakukan pemasangan *firewall*, sistem deteksi intrusi, dan pembaruan sistem dan perangkat lunak secara teratur untuk mengurangi kerentanan terhadap serangan siber.

**d. Pelatihan dan Kesadaran**

Bagian penting dari manajemen risiko *cyber security* adalah melibatkan awak kapal dalam pelatihan dan peningkatan kesadaran akan pentingnya keamanan teknologi informasi. Pelatihan ini dapat mencakup pengenalan terhadap praktik keamanan yang baik, identifikasi serangan siber, dan tindakan yang harus diambil dalam menghadapi ancaman. Kesadaran yang tinggi akan membantu dalam mencegah serangan dan melaporkan insiden yang mencurigakan.

**e. Pemantauan dan Respons**

Selanjutnya, penting untuk memantau sistem teknologi informasi secara terus-menerus guna mendeteksi adanya serangan atau aktivitas mencurigakan. Pemantauan ini dapat dilakukan dengan menggunakan sistem deteksi intrusi atau alat pemantauan jaringan. Jika terjadi serangan, respons yang cepat dan tepat harus dilakukan, termasuk isolasi sistem yang terkena dampak, pencabutan akses, dan pemulihan sistem.

Upaya untuk melindungi data dan sistem dari ancaman keamanan *cyber*, MV. EVER OCEAN menggunakan *Symantec Endpoint Protection* untuk melindungi komputer dan jaringan dari berbagai ancaman keamanan, termasuk *virus, malware, spyware, ransomware*, dan serangan berbasis *web* lainnya. Berikut adalah beberapa fitur utama dari *Symantec Endpoint Protection*:

a. Proteksi *Antivirus*

Melindungi komputer dari infeksi virus dan *malware* dengan mendeteksi dan menghapus ancaman yang mencurigakan.

b. *Firewall*

Menyediakan *firewall* yang dapat dikonfigurasi untuk mengontrol lalu lintas jaringan dan mencegah akses yang tidak sah atau berbahaya.

c. Deteksi Intrusi

Mendeteksi aktivitas mencurigakan atau serangan yang mencoba masuk ke dalam jaringan dan memberi peringatan atau mengambil tindakan yang sesuai.

d. Perlindungan *Email* dan *Web*

Memindai *email* dan lalu lintas *web* untuk mengidentifikasi dan memblokir ancaman yang datang melalui *email* atau situs *web* berbahaya.

e. Manajemen Sentral

Memungkinkan administrator untuk mengelola semua aspek keamanan dari satu konsol pusat, termasuk pemantauan, konfigurasi, dan pembaruan.

f. Teknologi Heuristik:

Menggunakan teknologi heuristik untuk mendeteksi ancaman yang belum dikenal dengan menganalisis perilaku file dan program.

g. Pembaruan Otomatis:

Mengupdate definisi virus dan perangkat lunak secara otomatis untuk memastikan perlindungan terhadap ancaman terbaru.

h. Proteksi terhadap *Ransomware*

Memiliki fitur proteksi terhadap *ransomware* yang dapat mencegah dan mengatasi serangan *ransomware*.

Dalam *The Guidelines on Cyber Security Onboard Ships* (2020:1) bahwa pendekatan terhadap *cyber Risk Management* akan bersifat spesifik untuk perusahaan dan kapal, namun harus dipandu oleh persyaratan peraturan dan pedoman nasional, internasional, dan negara bendera yang relevan. Pada tahun 2017, Organisasi Maritim Internasional (IMO) mengadopsi resolusi MSC.428 (98) tentang *Maritime Cyber Risk Management* dalam *Safety Management System* (SMS). Resolusi tersebut menyatakan bahwa SMS yang disetujui harus mempertimbangkan *Cyber Risk Management* sesuai dengan tujuan dan persyaratan fungsional ISM

*Code* (*International Safety Management*). Resolusi ini juga mendorong administrasi untuk memastikan bahwa risiko siber ditangani dengan tepat dalam SMS selambat-lambatnya pada verifikasi tahunan pertama Dokumen Kepatuhan (*Document of Compliance/DoC*) perusahaan setelah 1 Januari 2021. Pada tahun yang sama, IMO mengembangkan pedoman-pedoman yang memberikan rekomendasi tingkat tinggi tentang manajemen risiko siber maritim untuk melindungi pelayaran dari ancaman dan kerentanan siber yang ada saat ini dan yang sedang berkembang. Seperti yang juga disoroti dalam pedoman IMO, *Cyber Risk Management* yang efektif harus dimulai dari tingkat manajemen senior. Manajemen senior harus menanamkan budaya *Cyber Risk Management* ke dalam semua tingkat dan departemen organisasi dan memastikan rezim tata kelola risiko siber yang holistik dan fleksibel, yang beroperasi secara terus menerus dan terus dievaluasi melalui mekanisme umpan balik yang efektif.

Selanjutnya dalam *The Guidelines on Cyber Security Onboard Ships* (2020:8) bahwa Resolusi IMO MSC.428(98) mengidentifikasi kebutuhan mendesak untuk meningkatkan kesadaran akan ancaman dan kerentanan risiko siber untuk mendukung pelayaran yang aman dan selamat, yang secara operasional tahan terhadap risiko siber. Dengan demikian, semua pemangku kepentingan maritim harus bekerja untuk melindungi pelayaran dari ancaman dan kerentanan siber yang muncul. Resolusi ini juga menegaskan bahwa SMS harus mempertimbangkan manajemen risiko siber sesuai dengan tujuan dan persyaratan fungsional dari ISM *Code*.

Sesi ke-101 Komite Keselamatan Maritim IMO (laporan dari pertemuan ini dapat ditemukan di dokumen IMO MSC 101/24), setuju bahwa aspek *Cyber Risk Management*, termasuk aspek keamanan fisik dari keamanan *cyber*, harus dibahas dalam Rencana Keamanan Kapal (SSP) di bawah ISPS *Code*; namun, hal ini tidak boleh dianggap sebagai mengharuskan perusahaan untuk membuat sistem manajemen keamanan *cyber* yang terpisah yang beroperasi secara paralel dengan Sistem Manajemen Keselamatan (SMS) perusahaan.

Dalam pertemuan yang sama, IMO juga menegaskan bahwa resolusi MSC.428(98) tentang *Maritime Cyber Risk Management* dalam SMS

menetapkan persyaratan IMO untuk Administrasi untuk memastikan bahwa risiko *cyber* ditangani dengan tepat dalam SMS yang ada (seperti yang didefinisikan dalam ISM *Code*), diverifikasi oleh Dokumen Sertifikat Kepatuhan dan Manajemen Keselamatan yang telah disahkan, dan bahwa dalam Rencana Keamanan Kapal, referensi harus dibuat untuk prosedur manajemen risiko *cyber* yang ditemukan dalam SMS.

**4. Pengertian *Cyber Security***

Wahyu Tisno Atmojo (2021: 10) menyatakan bahwa *cyber security* adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi dan aset pengguna.

Perkembangan teknologi informasi juga telah memberikan perubahan signifikan mengenai konsep keamanan, kini ruang interaksi tidak bisa hanya dibatasi secara fisik tapi juga meluas ke dunia maya. Eko Budi (2021: 226). Perkembangan teknologi informasi telah mengubah konsep keamanan secara signifikan, memperluas ruang interaksi tidak hanya secara fisik tetapi juga ke dunia maya. Dalam era digital ini, keamanan menjadi sangat penting karena semakin banyaknya data yang disimpan dan diakses secara online.

Keamanan dalam konteks teknologi informasi mencakup perlindungan terhadap akses yang tidak sah, pembocoran data sensitif, serangan peretasan, dan ancaman lainnya yang dapat merusak integritas dan kerahasiaan informasi. Dalam dunia maya, ruang interaksi menjadi lebih kompleks karena adanya berbagai *platform* dan perangkat yang terhubung satu sama lain melalui jaringan komputer. Oleh karena itu, perlu adanya upaya untuk melindungi data dan sistem dari ancaman keamanan yang ada di dunia maya.. *Cyber security* tidak dapat diabstraksikan terlalu jauh dari wilayah aplikasinya dan lingkungan sosial-kultural, seperti dalam gambar berikut ini:


Gambar 2.1. Konsep *Cyber Security*

Terminologi “keamanan informasi (*information security*)” dan *cyber security* adalah dua konsep berbeda. Dalam konteks tertentu ada kesamaan pemahaman jika dikaitkan dengan proteksi aset atau perlawanan terhadap spionase industri dan ekonomi, perlawanan terhadap terorisme atau kejahatan ekonomi, perlawanan terhadap konten-konten terlarang.

Dalam konteks lain, dua konsep tadi memiliki perbedaan. *Cyber security* mencakup segala sesuatu berhubungan dengan pengawasan komputer, monitoring sampai kontrol yang sangat ketat atau perjuangan untuk hak asasi fundamental. Sedangkan keamanan informasi berhubungan dengan isu-isu yang lebih luas, seperti kedaulatan negara, keamanan nasional, proteksi atas infrastruktur penting, keamanan aset-aset yang terlihat maupun yang tidak terlihat, dan proteksi data personal dan sebagainya.

## 5. Pengertian *Society* 5.0

Wang (2018: 6) menyatakan bahwa *Society* 5.0 adalah kecerdasan paralel, yaitu merupakan suatu metodologi baru perluasan dari teori kecerdasan buatan tradisional kedalam *cyber*-fisik- sistem sosial (CPSS) yang muncul. Lebih khusus, kecerdasan paralel sangat efektif dalam menangani masalah tipe issue "manusia-dalam-*loop*" dengan kompleksitas sosial dan kompleksitas teknik, dan bertujuan mencari solusi cerdas, fokus, dan konvergen untuk masalah yang tidak pasti, beragam, dan kompleks.

Dengan menggunakan kecerdasan paralel, sistem komputer dapat mengeksplorasi berbagai solusi dengan cepat, menganalisis data yang tidak pasti, beragam, dan kompleks, dan menemukan solusi cerdas, fokus, dan konvergen untuk masalah yang dihadapi. Pendekatan ini sangat berguna

dalam situasi yang membutuhkan pemahaman mendalam tentang faktor sosial dan teknis yang saling terkait, serta memerlukan pemecahan masalah yang kompleks dan tidak terduga. Dengan menerapkan kecerdasan paralel, organisasi dapat mengoptimalkan proses pengambilan keputusan, meningkatkan efisiensi, dan menghadapi tantangan yang kompleks dengan solusi yang lebih baik.

### 6. Teori *Cyber Attack*

Koh, B. (t.t.): Richard A. Clarke and Robert K. Knake (2010: 3) menjelaskan bahwa *malware* adalah setiap kode komputer yang dapat digunakan untuk mencuri data, melewati kontrol akses, serta menimbulkan bahaya terhadap atau merusak *system*. Dalam *cyber attack*, selain virus, terdapat beberapa jenis serangan *malware* antara lain:

#### a. *Spyware* yang Melacak Aktivitas, Pengumpul Penekanan Tombol, dan Pengambilan Data.

*Spyware* adalah jenis program berbahaya yang dirancang untuk melacak aktivitas pengguna di perangkat komputer atau perangkat lunak. *Spyware* dapat mencatat dan mengumpulkan informasi seperti penekanan tombol, riwayat *browsing*, dan data pribadi pengguna tanpa sepengetahuan atau izin mereka. Data yang dikumpulkan oleh *spyware* kemudian dapat digunakan untuk tujuan yang tidak etis, seperti pencurian identitas, penipuan, atau pelanggaran privasi. *Spyware* sering kali tersembunyi di dalam program atau unduhan yang tampak sah, dan dapat menyebabkan kerugian serius bagi pengguna dan organisasi jika tidak terdeteksi dan dihapus dengan cepat.

#### b. *Adware* Dirancang untuk Menampilkan Iklan Namun Juga Ditemukan Membawa *Spyware*.

*Adware* adalah jenis perangkat lunak yang dirancang untuk menampilkan iklan kepada pengguna, sering kali dalam bentuk *pop-up* atau *banner* yang muncul saat menjelajah internet atau menggunakan aplikasi. Tujuan utama *adware* adalah untuk menghasilkan pendapatan melalui iklan yang ditampilkan. Namun, ada beberapa kasus di mana *adware* juga dapat membawa komponen *spyware* yang tidak diinginkan.

Komponen *spyware* ini dapat mengumpulkan data pengguna, seperti riwayat *browsing*, preferensi, atau informasi pribadi lainnya, dan mengirimkannya kepada pihak yang mengendalikan *adware*. Dalam beberapa situasi, *adware* yang membawa spyware dapat menjadi ancaman serius terhadap privasi dan keamanan pengguna.

**c. *Bot* yang Dirancang Otomatis Melakukan Tindakan Tertentu Secara *Online*.**

*Bot* adalah program komputer yang dirancang untuk melakukan tindakan tertentu secara otomatis di lingkungan *online*. *Bots* dapat digunakan untuk berbagai tujuan, baik yang positif maupun negatif. *Bots* yang digunakan dengan tujuan positif sering digunakan dalam pengelolaan media sosial, seperti merespons pesan atau mengelola postingan secara otomatis. Namun, ada juga bot yang dirancang untuk melakukan tindakan yang merugikan, seperti spamming, mencuri data, atau menyebarkan konten yang tidak diinginkan. *Bot-bot* ini dapat menyebabkan gangguan, merusak reputasi, atau bahkan menyebabkan kerugian finansial.

**d. *Ransomware* yang Mengenkripsi Data di Komputer dengan Kunci yang Tidak Diketahui oleh Pengguna.**

*Ransomware* adalah jenis serangan berbahaya yang bertujuan untuk mengenkripsi data yang ada di komputer atau sistem dengan menggunakan kunci yang tidak diketahui oleh pengguna. Setelah data terenkripsi, para penyerang akan meminta tebusan dalam bentuk uang atau *cryptocurrency* untuk memberikan kunci dekripsi yang diperlukan untuk mengembalikan akses ke data. *Ransomware* dapat menyebar melalui berbagai cara, termasuk melalui *email phishing*, situs *web* yang telah diretas, atau melalui *exploit* di jaringan yang rentan. Serangan ini dapat menyebabkan kerugian finansial yang signifikan, kehilangan data penting, dan gangguan operasional yang serius. Untuk melindungi diri dari serangan *ransomware*, penting untuk memiliki kebijakan keamanan yang kuat, menjaga perangkat lunak dan sistem operasi terbaru, melakukan *backup* data secara teratur, serta mengedukasi pengguna tentang praktik keamanan *online* yang aman.

## 7. Pengertian Virus

Menurut Yuni Selvita Suci (2018: 86), secara umum virus komputer merupakan sebuah *software* berbahaya (*malware*) yang dapat menyalin dirinya sendiri dan menyebar dengan cara menginfeksi/menyisipkan salinanya kedalam program maupun menyebarkkan program lain yang dapat di eksekusi. Beberapa kemampuan dasar virus, diantaranya adalah:

a. Kemampuan untuk memperbanyak diri.
b. Kemampuan menyembunyikan diri.
c. Kemampuan untuk memanipulasi.
d. Kemampuan mendapatkan informasi.
e. Kemampuan untuk memeriksa keberadaan dirinya.

Penggolongan atau pengelompokkan terhadap virus dapat dilakukan dengan beberapa metode klasifikasi. Beberapa metode yang sangat bagus menggunakan *naïve bayes* antara lain digunakan dalam klasifikasi deteksi email *spam*. Beberapa kemampuan dasar *worms*, di-antaranya adalah:

a. Kemampuan memperbanyak diri, yaitu kemampuan dasar suatu *worms* untuk menggandakan dirinya dan menyebar pada sistem komputer melalui perantara media lain seperti *disket*, USB *drive*, maupun melalui suatu jaringan komputer.
b. Kemampuan rekayasa sosial, yaitu kemampuan dasar suatu worms untuk mengelabuhi user dengan cara berpura-pura seperti program biasa. Ketika user menjalankan program tersebut maka secara otomatis *worms* tersebut akan aktif.
c. Kemampuan menyembunyikan diri, yaitu kemampuan suatu *worms* untuk menyembunyikan dirinya ketika *worms* sedang aktif sehingga user tidak mengetahui keberadaan *worms* tersebut.
d. Kemampuan mendapatkan informasi, yaitu kemampuan dasar sebuah *worms* untuk memperoleh informasi yang ia butuhkan, seperti jenis sistem operasi, direktori *system windows*, memeriksa *antivirus* dan lain sebagainya.

e. Kemampuan mengadakan manipulasi, yaitu kemampuan suatu *worms* untuk memanipulasi *registry* agar *worms* dapat aktif saat komputer dihidupkan, bahkan *worms* dapat memanipulasi *registry* milik suatu *antivirus* agar tidak menganggu *worms* tersebut.

Virus *cryptocurrency miner* menggunakan sumber daya komputer tanpa sepengetahuan pengguna. Hal ini mengakibatkan kinerja komputer yang melambat dan menyebar ke banyak komputer di jaringan kapal. Virus menghabiskan sumber daya komputer seperti memori, yang menyebabkan penurunan kinerja sistem. Virus *cryptocurrency miner* masuk ke dalam komputer melalui berbagai metode seperti lampiran email yang berbahaya, unduhan dari situs web yang tidak aman, atau melalui eksploitasi celah keamanan dalam sistem operasi atau perangkat lunak lainnya. Dalam kasus ini, virus tersebut masuk ke komputer melalui laptop pribadi yang terinfeksi yang terhubung ke jaringan kapal.

Setiap insiden siber harus dinilai untuk memperkirakan dampaknya terhadap operasi, aset, dan lain-lain. Dalam sebagian besar kasus hilangnya sistem TI, termasuk pelanggaran data terhadap informasi rahasia, akan menjadi bencana besar. masalah kelangsungan bisnis dan biasanya tidak berdampak langsung dan signifikan terhadap keselamatan pengoperasian kapal. Jika terjadi insiden dunia maya yang hanya memengaruhi sistem TI, prioritasnya adalah memberi tahu orang-orang yang ditunjuk di dalam kapal atau perusahaan yang mengoperasikan kapal untuk mendapatkan tanggapan segera, dan implementasi segera dari rencana investigasi dan pemulihan. Personil yang ditunjuk ini harus siap sedia jika terjadi insiden seperti itu.

Virus *cryptocurrency miner* yang menyebar ke banyak komputer di jaringan kapal dapat memiliki dampak serius terhadap operasional kapal. Beberapa dampak yang terjadi adalah sebagai berikut:

a. Virus tersebut akan menggunakan sumber daya komputer seperti memori dan daya pemrosesan untuk melakukan *cryptocurrency miner* tanpa sepengetahuan pengguna atau operator kapal. Hal ini akan mengakibatkan penurunan kinerja sistem komputer yang terinfeksi. Kinerja sistem yang melambat dapat mengganggu aktivitas sehari-hari, termasuk pemrosesan data, komunikasi, dan tugas-tugas lainnya.

b. Virus tersebut dapat menyebar melalui jaringan kapal dan menginfeksi banyak komputer secara simultan. Hal ini dapat menyebabkan gangguan pada jaringan kapal, seperti penurunan kecepatan jaringan, koneksi yang terputus, atau bahkan kegagalan jaringan.

c. Virus tersebut dapat memanfaatkan celah keamanan dalam sistem operasi atau perangkat lunak lainnya untuk masuk ke dalam komputer. Dalam proses ini, virus bisa mengungkapkan kerentanan keamanan yang lebih luas di kapal. Jika virus dapat memanfaatkan celah keamanan untuk memasuki komputer, kemungkinan besar ada potensi bagi pihak yang tidak berwenang untuk juga memanfaatkannya. Hal ini dapat membahayakan keamanan data dan informasi penting di kapal.

## 8. *Standard Operating Procedure* (SOP)

### a. Definisi *Standard Operating Procedure* (SOP)

Menurut Arini T. Soemohadiwidjojo (2014: 90), *Standard Operating Procedure* (SOP), atau disebut juga sebagai ”Prosedur” adalah dokumen yang lebih jelas dan rinci untuk menjabarkan metode yang digunakan dalam mengimplementasikan dan melaksanakan kebijakan dan aktivitas produksi seperti yang ditetapkan dalam pedoman. Pada dasarnya, prosedur merupakan instruksi tertulis sebagai pedoman dalam menyelesaikan sebuah tugas rutin atau tugas yang berulang dengan cara yang efektif dan efisien, untuk menghindari terjadinya variasi atau penyimpangan yang dapat mempengaruhi kinerja organisasi secara keseluruhan.

Standar Operasional Prosedur yang baik adalah prosedur yang memiliki informasi dan langkah-langkahnya dapat dipahami secara akurat, sehingga memfasilitasi terjadinya ketaatan terhadap lingkungan. SOP sebaiknya dibuat dengan melihat aktivitas yang berlangsung di lapangan, kemudian aktivitas tersebut dibuat dan disusun berdasarkan hal-hal yang terjadi di lapangan. Perlu dipahami bahwa tidak semua elemen organisasi melakukan SOP.

**b. Prosedur Penanganan Insiden *Malware***

Dalam Panduan Penanganan Insiden *Malicious Software* (*Malware*) (2018: 6), prosedur penanganan terhadap insiden *malware* dapat dilakukan dalam beberapa tahap seperti pada gambar berikut:


Gambar 2.2. Tahap penanganan insiden

**1) Persiapan**

Persiapan tahap ini adalah tahap dimana kebijakan, prosedur, teknologi, dan sumber daya manusia harus disiapkan secara matang, dimana akan digunakan pada proses penanganan terhadap insiden. Dalam suatu organisasi/institusi, kemampuan melakukan respon yang cepat terhadap suatu insiden, merupakan persiapan yang mendasar bagi penanganan insiden yang disebabkan oleh *malware*. Langkah-langkah yang diambil pada tahap ini antara lain:

a) Pembentukan Tim Respon Tim dapat berasal dari internal organisasi/institusi atau jika memang diperlukan dapat berasal dari luar organisasi/institusi (eksternal). Anggota tim memiliki pengetahuan tentang *malware* dan memiliki kemampuan penanganan insiden *malware*.

b) Penyiapan Dokumen Legal. Menyiapkan dokumen yang dibutuhkan dalam proses penanganan insiden *malware*. Dokumen ini antara lain:

(1) Panduan Penanganan Insiden Siber

(2) Formulir Penanganan Insiden Siber

(3) Dokumen Kebijakan, diantaranya kebijakan keamanan, kebijakan pengunaan laptop, *antivirus*, internet dan *email*, serta kebijakan *backup*.

(4) Dokumen Baseline *Performance*.

(5) Dokumen Audit Sistem.

(6) Dokumen Profil dari semua perangkat lunak dan proses-proses yang harus berjalan pada sistem berdasarkan proses bisnis organisasi.

(7) *Database* penanganan insiden yang pernah terjadi sebelumnya.

(8) Daftar yang memuat indikasi-indikasi suatu komputer atau jaringan terkena *malware*, misalkan daftar aplikasi yang telah terindikasi terkena *malware*, alamat IP terkait dengan *Command and Control* (C&C).

c) Menentukan tempat (ruangan) untuk penanganan.

d) Menentukan lingkungan yang aman untuk analisa *malware* agar dampak *malware* tidak menyebar ke sistem yang lain.

e) Menyiapkan *tools* yang akan digunakan, diantaranya:

(1) *Tools* untuk penyaringan, misalnya :

(a) *Squid* merupakan perangkat lunak *open source* pada *web proxy* yang mendukung filter URL;

(b) *Squid Guard* adalah *tools* yang dapat digunakan untuk menyederhanakan tugas filter URL yang merupakan plug-in untuk squid yang merupakan kombinasi dari filter, *redirector*, dan akses kontrol, yang dapat digunakan untuk membuat aturan akses berdasarkan pada waktu, kelompok pengguna, dan URL.

(2) *Tools* untuk menghitung nilai *hash*.

(3) *Tools* untuk deteksi virus baik berbasis *host* maupun *online*, misalnya *antivirus* dan *website* *www.virustotal.com*

(4) *Tools* pendeteksi berbasis *host*, misalnya Samhain, OSSEC dan Osiris.

f) *Tools* untuk analisa *malware*, meliputi :

1) Mesin uji, merupakan mesin virtual untuk melakukan analisis terhadap *malware*, misalnya VMWare, MS VPC, dan Xen. Mesin uji ini diperlukan dalam melakukan analisa *malware* menggunakan metode analisa dinamis.

2) *Utility toolkit*, *tools* ini digunakan untuk mengumpulkan sampel untuk analisis *malware* atau untuk mengidentifikasi, menampung, dan memberantas *malware*, misalnya *SysInternals*.

3) *Reverse Engineering tools*, merupakan *tools* yang digunakan untuk melakukan analisa lebih lanjut terkait *source code* dari sampel *malware*, misalnya IDA-*Pro*, CFF *Explorer*, dan *WinHex*. *Reverse Engineering tools* diperlukan dalam melakukan analisa *malware* menggunakan metode analisa statis.

**2) Identifikasi dan Analisis**

Tahap ini merupakan tahap identifikasi adanya *malware*. Proses-proses yang dilakukan dalam tahap identifikasi adalah sebagai berikut :

a) Memeriksa apakah *antivirus* berfungsi normal atau tidak. Hal ini karena ada *malware* yang dapat menghancurkan instalasi *antivirus* dengan merusak *executable file*, mengubah kunci registri atau merusak file definisi, maupun menonaktifkan *update* dari *signature* suatu file.

b) Mengecek file yang tidak dikenal pada *root* atau *system directory*.

c) Memeriksa file dengan ekstensi ganda. Sangat disarankan untuk menonaktifkan opsi fitur 'sembunyikan ekstensi' pada *file explorer* untuk mengetahui ekstensi yang sebenarnya dari suatu file.

d) Memeriksa proses dan *service* yang tidak dikenal dalam sistem menggunakan *Task Manager*

e) Memeriksa utilitas sistem, misalnya *Task Manager* atau *SysInternals Process Explorer*. Terdapat *malware* yang menonaktifkan utilitas ini sehingga tidak dapat dijalankan.

f) Memeriksa penggunaan *memory* CPU menggunakan *Task Manager*.

g) Memeriksa anomali pada *Registry Key*.

h) Memeriksa anomali pada *traffic* jaringan. *Malware* modern saat ini kebanyakan memiliki fitur "*Command and Control*" dimana biasanya setiap *malware* yang sudah menginfeksi suatu sistem, akan mengirimkan sinyal kepada induk *malware* melalui aktivitas "*Command and Control*" tersebut.

i) Identifikasi anomali proses dan *service* yang dibuat pada *Task Scheduler*.

j) Identifikasi *user account* pada sistem. Beberapa *malware* mempunyai kemampuan untuk membuat *user account* baru pada sistem operasi yang terinfeksi.

k) Identifikasi *entry log* pada sistem operasi menggunakan *Event Viewer*.

l) Identifikasi proses yang mencurigakan menggunakan *SysInternals Tools. SysInternal Tools* merupakan salah satu kumpulan *tools* utilitas milik *Microsoft* yang bertujuan untuk mengidentifikasi sistem lebih mendetail. Beberapa Aplikasi *SysInternal tools* yang paling banyak digunakan untuk melakukan identifikasi dan analisa *malware* adalah *Process Explorer*, *Autoruns*, dan *Process Monitor*.

**3) *Containment***

Tahap ini bertujuan untuk menghentikan atau mencegah penyebaran *malware*. Prosedur yang dilakukan pada tahap *containment* adalah sebagai berikut :

a) Meminta izin kepada pemilik sistem untuk memutus sistem yang terinfeksi *malware* dari jaringan.

b) Isolasi sistem yang terinfeksi *malware*. Hal ini dapat dilakukan dengan cara mencabut kabel LAN atau memindahkan sistem tersebut ke VLAN khusus. Namun, perlu menyimpan informasi koneksi jaringan pada sistem sebelum

c) memutuskan hubungan dari jaringan yang mungkin akan dibutuhkan dalam melakukan analisa selanjutnya.

d) Mengubah konfigurasi *routing table* pada *Firewall* untuk memisahkan sistem yang terinfeksi *malware* dengan sistem lainnya.

e) Melakukan *backup data* pada sistem yang terinfeksi *malware*. Identifikasi gejala kemiripan pada sistem lain untuk mencegah penyebaran *malware*. Jika terdapat kemiripan, maka sistem tersebut juga harus dilakukan proses *containment*.

**4) *Eradication***

Tahap ini merupakan tahapan dimana beberapa teknik yang berbeda-beda digunakan untuk melakukan analisa terhadap *malware* dan menghapus *malware* dari sistem yang telah terinfeksi. Setelah *file* yang terinfeksi diidentifikasi, gejala *malware* dicatat dan *executable malware* diidentifikasi dan dianalisis, kemudian semua *file executables malware* dan artefak yang ditinggalkan oleh *malware* akan dihapus, serta menutup *port* yang terindikasi sebagai lubang masuknya *malware*. Proses-proses yang dilakukan dalam tahap ini adalah sebagai berikut :

a) Menghentikan proses yang terindikasi sebagai proses yang *malicious*, dengan cara sebagai berikut :

(1) Tidak melakukan *kill* / *end process* terhadap *malicious* process tersebut. Hal ini dikarenakan *malware* akan melakukan *autostart process* ketika prosesnya terhenti.

(2) Lakukan *suspend* terhadap proses tersebut, kemudian lakukan *record* pada path *EXE* proses tersebut dan *file* DLL yang dipanggil oleh proses tersebut.

(3) Dalam kondisi *sleep* (proses di *suspend*), kemudian satu persatu lakukan *kill process* dari kumpulan *malicious process* tersebut dimulai dari child *process* ke *parent process*.

(4) Jika *malicious process* masih melakukan *autostart* atau mengganti Namanya dengan nama proses baru, maka perlu didokumentasikan lebih lanjut dan simpan *malicious program* tersebut ke media lain untuk proses analisa yang lebih mendetail.

b) Menghapus *autostart process* yang mencurigakan dari hasil analisa aplikasi *autostart*.

c) Jika proses tersebut kembali lagi, jalankan *Process Monitor* untuk mengidentifikasi apakah ada lokasi lain dimana *malware* tersebut bersembunyi.

d) Lakukan proses di atas secara berulang hingga dapat dipastikan semua *malicious* program telah dihapus dan prosesnya sudah di *kill process*.

e) Setelah program *malware* dihapus dan mal*icious process* di *kill process*, lakukan *full scanning* terhadap sistem menggunakan *signature antivirus* yang sudah diperbaharui.

f) Jika proses *scanning antivirus* tidak dapat dilakukan karena telah diblokir oleh *malware*, maka lakukan proses sebagai berikut :

(1) *Booting* sistem melalui *Live usb rescue disk*, misalnya *Hiren Boot* CD, *FalconFour's Ultimate Boot* CD, *Kaspersky Rescue Disk*, dan lain-lain.

(2) *Live* USB tersebut dapat berupa sistem operasi *Linux* ataupun *miniXP* yang berisi beberapa *tools* seperti *defragment tools, driver tools, backup* dan *recover data tools, antivirus* dan *anti-malware tools*, rootkit *detection tools, secure data wiping tools, partitioning tools, password recovery tools, network tools, recover/repair broken partitions tools*, dan

lain-lain. Lakukan proses *mounting* sistem operasi yang terinfeksi ke dalam *Live* USB yang sedang berjalan.

(3) Lakukan proses *scanning antivirus* dan *antimalware* pada *Live* USB yang sedang berjalan

g) Jika terdapat *user-user* yang dibuat oleh *malware*, maka hapus *user-user* yang tidak dikenali tersebut untuk menghindari masuknya kembali *malware* melalui *user* yang tidak dikenal tersebut.

**5) Pemulihan**

Pemulihan merupakan tahap untuk mamulihkan data sistem yang terinfeksi *malware* serta mengembalikan seluruh sistem bekerja normal seperti semula. Langkah yang dilakukan terhadap pemulihan sistem, diantaranya:

a) Validasi sistem untuk memastikan sudah tidak ada aplikasi atau *file* yang rusak atau terinfeksi *malware*. Begitu pula kesalahan atau kekurangan konfigurasi sistem untuk kemudian disesuaikan kembali.

b) Melakukan aktivitas *monitoring* untuk memastikan apakah *malware* masih ada atau kembali lagi setelah proses *eradication* dengan malakukan hal-hal sebagai berikut :

(1) Memantau proses dan servis yang berjalan menggunakan *Process Monitor* dan *Process Explorer*.

(2) Memantau aktivitas traffic jaringan menggunakan *tools wireshark* atau *tcpdump* untuk memantau apakah ada *request outgoing* atau *traffic incoming* yang mencurigakan, serta *request query* DNS karena *malware* yang memiliki kemampuan *Command and Control* biasanya melakukan kontak dengan induknya.

c) Jika terjadi kerusakan yang cukup parah (*file* sistem terhapus, data penting hilang, menyebabkan kegagalan *booting* pada sistem

operasi), maka sistem dibangun ulang dari *file backup* terakhir sistem yang dimiliki.

d) Melakukan *patching* sistem.

e) Melakukan *hardening* terhadap sistem.

f) Menambahkan *signature* dari *malware* ke sistem *monitoring* atau *database antivirus*.

**6) Tindak Lanjut**

Tahap ini adalah fase di mana semua dokumentasi kegiatan yang dilakukan dicatat sebagai referensi untuk masa mendatang. Prosedur yang dapat dilakukan adalah sebagai berikut:

a) Membuat dokumentasi dan laporan terkait penanganan insiden *malware*, yang berisi langkah-langkah dan hasil yang telah didapatkan.

b) Memberikan analisa dan penjelasan apa yang harus dilakukan, sehingga meminimalisir insiden serupa tidak terulang kembali.

c) Menuliskan bukti-bukti yang ditemukan, hal ini terkait dengan proses hukum kedepannya.

d) Membuat evaluasi dan rekomendasi. Rekomendasi yang dapat diberikan diantaranya:

(1) Penambahan pengetahuan tentang penanganan insiden *malware*, misalnya melalui pelatihan

(2) Memperbaharui anti *malware* dengan *signature file* yang baru, dengan harapan dapat berhasil dalam mendeteksi dan menghapus *malware*

(3) Meningkatkan pertahanan sistem terhadap *malware*

e) Mendokumentasikan *malware* terkait jalan masuk, perilaku, dampak kerusakan, dan lain-lain yang terkait *malware* ke dalam *database malware*.

f) Menyempurnakan langkah-langkah respon atau prosedur penanganan insiden *malware* yang ada.

**9. *Contingency Plans***

Dalam *Cyber-Security-Guidelines Onboard Ships* (2020: 41), sebuah *contingency plans* harus dikembangkan yang mencakup kemungkinan-kemungkinan darurat yang relevan, dan semua rencana harus disimpan dalam bentuk cetak jika terjadi kehilangan akses elektronik terhadap rencana tersebut. Saat mengembangkan *contingency plans* untuk penerapan di kapal, penting untuk memahami pentingnya setiap insiden *cyber* sebagai masalah keselamatan dan memprioritaskan tindakan respons yang sesuai. Hal ini hanya dapat dicapai bersama dengan tim dari manajemen.

Berikut ini adalah contoh daftar insiden *cyber* yang harus ditangani dalam *contingency plans*:

a. Hilangnya ketersediaan peralatan navigasi elektronik atau hilangnya integritas data terkait navigasi

b. Hilangnya ketersediaan atau integritas sumber data eksternal, termasuk namun tidak terbatas pada GNSS

c. Hilangnya konektivitas penting dengan darat, termasuk namun tidak terbatas pada ketersediaan *Global Maritime Distress and Safety System* (GMDSS).

d. Hilangnya ketersediaan sistem termasuk sistem propulsi, sistem bantu, dan sistem penting lainnya, serta hilangnya integritas pengelolaan dan pengendalian data.

e. Terjadi *Ransomware* atau insiden penolakan layanan.

*Contingency plans* dan informasi terkait harus mencakup komunikasi dan manajemen eskalasi untuk memastikan bahwa dukungan berbasis darat yang tepat dapat diakses, dan harus tersedia dalam bentuk non-elektronik karena beberapa jenis insiden *cyber* dapat mencakup penghapusan data dan penutupan jalur komunikasi.

*Contingency plans* harus dirancang dengan hati-hati, dan personel yang ditunjuk di darat harus diintegrasikan dengan kapal jika terjadi insiden *cyber*. Nakhoda dan petugas yang ditunjuk harus diberikan rencana ini untuk memungkinkan pelatihan dan peninjauan berkala agar lebih familiar.

Dalam mengembangkan *contingency plans* untuk penerapan di kapal terkait dengan insiden keamanan *cyber*, berikut adalah beberapa langkah yang dapat diambil:

a. Identifikasi dan penilaian risiko

Tim manajemen kapal harus melakukan identifikasi dan penilaian risiko terkait dengan insiden keamanan *cyber*. Ini melibatkan mengidentifikasi potensi ancaman dan kerentanan yang mungkin timbul di lingkungan operasional kapal, serta mengevaluasi dampak dan probabilitas terjadinya insiden tersebut. Dengan pemahaman yang jelas tentang risiko yang ada, langkah-langkah respons yang tepat dapat ditentukan.

b. Pembentukan tim respons keamanan *cyber*

Bentuklah tim respons keamanan *cyber* yang terdiri dari anggota yang terlatih dan berpengalaman dalam bidang keamanan komputer. Tim ini harus memiliki pengetahuan dan keterampilan yang diperlukan untuk mengatasi insiden keamanan *cyber* secara efektif. Mereka juga harus diberi wewenang dan sumber daya yang cukup untuk menangani insiden dan mengkoordinasikan respons.

c. Penetapan tindakan respons

Bersama dengan tim respons keamanan *cyber*, identifikasi dan tetapkan tindakan respons yang harus diambil dalam berbagai skenario insiden keamanan *cyber*. Tindakan ini harus mencakup upaya mitigasi, pemulihan, dan pengendalian insiden. Misalnya, tindakan respons dapat meliputi isolasi sistem terinfeksi, pemulihan dari cadangan data yang sah, perbaikan kerentanan yang dieksploitasi, dan peningkatan keamanan sistem.

d. Komunikasi dan koordinasi

Pastikan ada saluran komunikasi yang jelas dan efektif antara tim respons keamanan *cyber*, manajemen kapal, dan personel lain yang terlibat dalam respons insiden. Koordinasi yang baik sangat penting

dalam menghadapi insiden keamanan *cyber*, termasuk komunikasi yang tepat waktu, pertukaran informasi, dan pembagian tugas yang jelas.

e. Pemulihan dan evaluasi

Setelah insiden keamanan *cyber* teratasi, lakukan pemulihan penuh sistem dan infrastruktur yang terkena dampak. Selanjutnya, lakukan evaluasi menyeluruh terhadap insiden tersebut untuk mengidentifikasi kelemahan dalam sistem keamanan yang ada dan mengevaluasi keefektifan langkah-langkah respons yang diambil. Hasil evaluasi ini harus digunakan untuk meningkatkan kebijakan keamanan dan langkah-langkah pencegahan di masa depan.

f. Pelatihan dan kesadaran

Selenggarakan pelatihan rutin untuk awak kapal dan personel terkait untuk meningkatkan kesadaran mereka tentang ancaman keamanan *cyber* dan langkah-langkah yang harus diambil dalam merespons insiden. Pelatihan ini harus mencakup pengenalan terhadap tindakan pencegahan, deteksi dini, dan respons yang tepat terhadap serangan keamanan *cyber*.

g. Penyimpanan rencana dalam bentuk cetak

Rencana respons keamanan *cyber* yang dikembangkan harus disimpan dalam bentuk cetak sebagai langkah kontinjensi jika terjadi kehilangan akses elektronik di kapal. Hal ini memastikan bahwa rencana tersebut tetap dapat diakses dan diimplementasikan bahkan jika terjadi gangguan pada sistem elektronik.

## 10. Pengertian Pelatihan

Menurut Sari (2018:101), pelatihan adalah semua usaha untuk memyediakan memperoleh, meningkatkan, dan mempertahankan keterampilan kerja, hasil barang yang dikeluarkan, sikap, serta etika pada jenjang kemampuan serta skill tertentu, sesuai sesuai dengan standar serta kualifikasi jabatan serta pekerjaan.

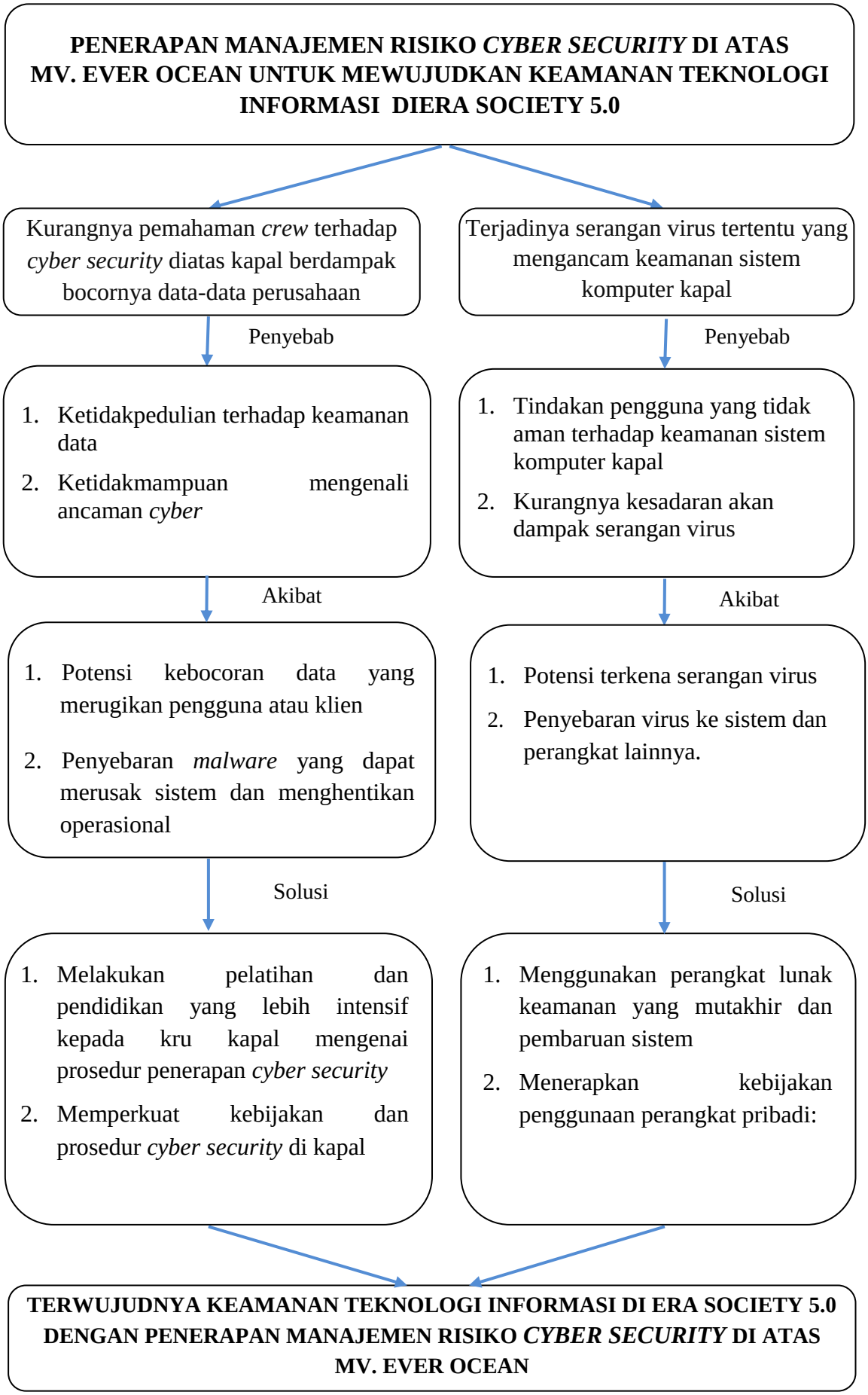
Pelatihan merupakan salah satu strategi yang harus dilakukan untuk memperkuat keamanan siber (*cyber security*) dan mewujudkan keamanan

di era *Society* 5.0. Pelatihan ini bertujuan untuk meningkatkan kemampuan dan pengetahuan sumber daya manusia dalam menghadapi ancaman keamanan siber. Pelatihan dalam bidang keamanan siber sangat penting karena keamanan siber melibatkan berbagai aspek, termasuk pemahaman tentang teknologi, kebijakan, prosedur, dan praktik terbaik dalam mengelola risiko keamanan siber. Dalam pelatihan ini, para ahli keamanan siber akan melatih individu-individu untuk mengidentifikasi ancaman keamanan, mencegah serangan siber, dan merespon dengan cepat dan efektif jika serangan terjadi.

Pelatihan juga penting untuk meningkatkan pemahaman tentang undang-undang dan regulasi terkait keamanan siber. Dalam hal ini, pelatihan akan membantu individu dan organisasi untuk memahami kewajiban hukum yang terkait dengan keamanan siber, serta langkah-langkah yang harus diambil dalam melindungi data sensitif dan informasi penting dari serangan siber. Selain itu, pelatihan juga dapat membantu meningkatkan kerja sama dan kolaborasi antara pemangku kepentingan domestik dan internasional di bidang keamanan siber. Pelatihan ini memungkinkan para peserta untuk berbagi pengetahuan, pengalaman, dan praktik terbaik dalam menghadapi ancaman keamanan siber yang semakin kompleks dan terus berkembang. Dengan melakukan pelatihan yang efektif, baik dalam bentuk pelatihan teknis maupun pelatihan kesadaran keamanan siber, dapat meningkatkan kemampuan dan kesiapan dalam menghadapi ancaman keamanan siber, melindungi infrastruktur teknologi informasi, serta menjaga keamanan di era *Society* 5.0.

## B. KERANGKA PEMIKIRAN

Kerangka pemikiran membantu mengarahkan alur naratif penulisan dengan cara yang logis dan kohesif. Ini memungkinkan pembaca untuk mengikuti argumen secara sistematis dan memahami bagaimana setiap elemen terkait dengan yang lainnya. Dengan merinci batasan masalah, penyebab, akibat, penyelesaian, dan keluaran, penulis dapat membentuk argumen yang kuat dan komprehensif, serta menyampaikan informasi kepada pembaca.


PENERAPAN MANAJEMEN RISIKO CYBER SECURITY DI ATAS MV. EVER OCEAN UNTUK MEWUJUDKAN KEAMANAN TEKNOLOGI INFORMASI DIERA SOCIETY 5.0
Kurangnya pemahaman crew terhadap cyber security diatas kapal berdampak bocornya data-data perusahaan
Terjadinya serangan virus tertentu yang mengancam keamanan sistem komputer kapal
Penyebab
Penyebab
1. Ketidakpedulian terhadap keamanan data
2. Ketidakmampuan mengenali ancaman cyber
1. Tindakan pengguna yang tidak aman terhadap keamanan sistem komputer kapal
2. Kurangnya kesadaran akan dampak serangan virus
Akibat
Akibat
1. Potensi kebocoran data yang merugikan pengguna atau klien
2. Penyebaran malware yang dapat merusak sistem dan menghentikan operasional
1. Potensi terkena serangan virus
2. Penyebaran virus ke sistem dan perangkat lainnya.
Solusi
Solusi
1. Melakukan pelatihan dan pendidikan yang lebih intensif kepada kru kapal mengenai prosedur penerapan cyber security
2. Memperkuat kebijakan dan prosedur cyber security di kapal
1. Menggunakan perangkat lunak keamanan yang mutakhir dan pembaruan sistem
2. Menerapkan kebijakan penggunaan perangkat pribadi:
TERWUJUDNYA KEAMANAN TEKNOLOGI INFORMASI DI ERA SOCIETY 5.0 DENGAN PENERAPAN MANAJEMEN RISIKO CYBER SECURITY DI ATAS MV. EVER OCEAN

# BAB III
# ANALISIS DAN PEMBAHASAN

## A. DESKRIPSI DATA

Peristiwa yang terjadi di atas MV. EVER OCEAN pada tanggal 5 Juni 2023 menunjukkan betapa pentingnya pemahaman tentang *cyber security* bagi seluruh kru kapal. Meskipun kapal dilengkapi dengan teknologi canggih dan sistem keamanan, serangan *phising* yang berhasil masuk ke sistem kapal mengungkapkan celah yang perlu diperhatikan.

Dalam peristiwa tersebut, seorang anggota kru secara tidak sengaja mengklik tautan mencurigakan dalam sebuah email. Hal ini merupakan contoh dari teknik serangan *phising* di mana penyerang mencoba untuk memperoleh informasi sensitif dengan menyamar sebagai entitas terpercaya. Saat *malware* berhasil masuk ke sistem kapal, dampaknya sangat merugikan perusahaan. Data-data penting seperti rute pelayaran, jadwal pengiriman, dan informasi pelanggan bocor ke pihak yang tidak bertanggung jawab.

Salah satu komputer terdeteksi terkena virus oleh *shore monitoring program* karena kru kapal menghubungkan laptop pribadi yang terinfeksi virus ke jaringan kapal, menyebabkan PC (*Personal Computer*) di dek kapal dan dua komputer umum yang tidak memperbarui *anti- virus definition* terinfeksi virus. Setelah dianalisis, virus tersebut diidentifikasi sebagai *cryptocurrency miner* untuk menyalin *malware* ke setiap *disk slot* dan menyebarluaskan melalui folder berbagi untuk terus menginfeksi lebih banyak komputer dan menyebarkan lebih banyak *cryptocurrency miner* setelah mendapatkan kesempatan untuk terhubung ke internet.

Virus *cryptocurrency miner* menggunakan sumber daya komputer tanpa sepengetahuan pengguna. Hal ini mengakibatkan kinerja komputer yang melambat dan menyebar ke banyak komputer di jaringan kapal. Virus menghabiskan sumber

daya komputer seperti memori, yang menyebabkan penurunan kinerja sistem. Virus *cryptocurrency miner* masuk ke dalam komputer melalui berbagai metode seperti lampiran email yang berbahaya, unduhan dari situs web yang tidak aman, atau melalui eksploitasi celah keamanan dalam sistem operasi atau perangkat lunak lainnya. Dalam kasus ini, virus tersebut masuk ke komputer melalui laptop pribadi yang terinfeksi yang terhubung ke jaringan kapal.

Selain itu menggunakan perangkat penyimpanan massal USB *(Universal Serial Bus*) di atas kapal terlihat tidak berbahaya karena kemudahan *Plug-and-Play*, tetapi berpotensi menimbulkan banyak masalah dan meningkatkan *cyber-risk* untuk semua sistem komputer di atas kapal. Berdasarkan laporan bahwa ada banyak sekali *malware* yang tersebar saat ini melalui perangkat USB. *Malware* yang telah ditemukan adalah *trickbot*, sebuah *trojan* yang menjadi ancaman. *Trojan* ini dirancang dengan tujuan mencuri informasi login dari pengguna yang terinfeksi. *TrickBot* menyebar melalui email *phishing* yang mengandung lampiran berbahaya atau tautan yang mengarah ke situs web palsu.

Selain itu penggunaan perangkat penyimpanan massal USB di atas kapal terlihat tidak berbahaya karena kemudahan *Plug-and-Play* yang memungkinkan pengguna untuk langsung menggunakan perangkat tersebut tanpa perlu instalasi khusus. Namun, fakta penggunaan perangkat USB oleh *crew* di atas kapal menimbulkan banyak masalah dan meningkatkan *cyber-risk* untuk semua sistem komputer di MV EVER OCEAN.

Dilaporkan *malware trickbot* yang tersebar melalui perangkat USB, menjadi perhatian serius dalam penggunaan perangkat penyimpanan massal di atas kapal. *Malware* dapat dengan mudah menyusup ke dalam perangkat USB dan menyebar ke sistem komputer saat perangkat tersebut terhubung. Penyebaran *malware trickbot* melalui perangkat USB menjadi ancaman serius dalam lingkungan penggunaan perangkat USB di atas kapal. *Malware* dengan mudah menyusup ke dalam perangkat USB dan menyebar ke sistem komputer saat perangkat tersebut terhubung. Ketika sebuah perangkat USB terinfeksi *malware*, menyebabkan masalah sistem yang serius pada komputer yang digunakan untuk memantau pengoperasian *main/auxiliary engines* dalam ruang mesin, sistem pemantauan *container*, *ballast water management system*, dan peralatan navigasi di anjungan.

Dengan terjadinya permasalahan di atas, perusahaan menetapkan peraturan manajemen perangkat penyimpanan massal USB untuk dipatuhi oleh seluruh armada perusahaan. Peraturan manajemen perangkat penyimpanan massal USB yang diterapkan oleh perusahaan tersebut sangat penting untuk menjaga keamanan data dan sistem. Berikut adalah penjelasan lebih lanjut mengenai peraturan-peraturan tersebut:

1. Dilarang mentransfer file tidak resmi dan *computer games* ke komputer umum kapal, laptop pribadi, dan komputer terhubung ke jaringan kapal:
2. Dilarang membagikan folder melalui jaringan kapal kecuali untuk PC dek folder berbagi:
3. Mengunduh definisi anti-virus terbaru secara berkala dan pastikan semua komputer umum yang terpasang telah diperbarui dengan baik:
4. Dilarang menjalankan, menyalin, menginstal, dan mengunduh perangkat lunak dan file yang tidak sah dengan menggunakan perangkat USB.
5. Data dan file yang disimpan dalam perangkat USB terdaftar harus dibatasi hanya untuk bisnis resmi, dilarang mencampur dengan file tidak resmi, perangkat lunak ilegal, *ebook*, permainan komputer, dan file audio-visual.
6. Memindai sepenuhnya secara teratur, status perlindungan *Symantec Endpoint* untuk semua komputer yang ada di dalam kapal.

## B. ANALISIS DATA

### 1. Kurangnya Pemahaman *Crew* Terhadap *Cyber Security* di Atas Kapal Berdampak Bocornya Data-Data Perusahaan

Kurangnya pemahaman *crew* terhadap *cyber security* di atas kapal berdampak pada bocornya data-data perusahaan. Hal ini karena *crew* yang tidak memahami tindakan pencegahan dan *cyber security* rentan terhadap serangan *malware trickbot.*

Penyebabnya adalah :

#### a. Ketidakpedulian Terhadap Keamanan Data

Ketidakpedulian terhadap keamanan data merupakan salah satu

faktor yang dapat terjadi akibat kurangnya pemahaman *crew* terhadap *cyber* security di atas kapal. Banyak *crew* yang tidak menyadari pentingnya menjaga keamanan data dan rentan terhadap tindakan yang dapat mengakibatkan bocornya data perusahaan. Mereka tidak mematuhi kebijakan keamanan yang telah ditetapkan, seperti menggunakan password yang lemah atau berbagi informasi sensitif melalui kanal yang tidak aman. Hal ini dapat menyebabkan data perusahaan menjadi rentan terhadap serangan dan penyalahgunaan oleh pihak yang tidak berwenang.

Data perusahaan bocor akibat ketidakpedulian terhadap keamanan data, hal ini menyebabkan konsekuensi yang merugikan bagi pengguna. Data yang bocor, seperti mencuri informasi login, dapat dimanfaatkan oleh pihak yang tidak berwenang. Bocornya informasi *login* dapat memberikan akses kepada pihak yang tidak berwenang ke akun pengguna, baik itu akun perusahaan maupun akun pengguna individu. Dampaknya mencakup pencurian identitas dan penyebaran *malware*.

**b. Ketidakmampuan Mengenali Ancaman *Cyber***

*Crew* yang tidak memiliki pemahaman yang memadai tentang taktik dan teknik yang digunakan oleh para penyerang *cyber* tidak akan mampu mengidentifikasi ancaman yang ada. Mereka tidak menyadari tanda-tanda serangan seperti upaya *phishing*, *malware*, atau serangan virus. Hal ini membuat mereka rentan terhadap serangan *cyber* yang mengakibatkan kebocoran data perusahaan. Penyebaran *malware* yang merusak sistem.

Berikut ini adalah tabel yang menjelaskan dampak dari kurangnya pemahaman *crew* terhadap taktik dan teknik yang digunakan oleh para penyerang *cyber*:

Tabel 3.1. Taktik dan Teknik Penyerang *Cyber*

| **Dampak Kurangnya Pemahaman *Crew* Terhadap Taktik dan Teknik Penyerang *Cyber*** | **Tanda-tanda Serangan yang Tidak Dikenali oleh *Crew*** |
|---|---|
| Tidak mampu mengidentifikasi serangan *phishing* | Email yang mencurigakan dan meminta informasi sensitif |

| Dampak Kurangnya Pemahaman *Crew* Terhadap Taktik dan Teknik Penyerang *Cyber* | Tanda-tanda Serangan yang Tidak Dikenali oleh *Crew* |
|---|---|
| Tidak menyadari adanya upaya *malware* | Perangkat lunak yang terasa lambat atau tidak berfungsi dengan baik |
| Tidak mengenali serangan *virus* | File atau lampiran yang mencurigakan |

Dalam tabel di atas, terlihat bahwa kurangnya pemahaman *crew* terhadap taktik dan teknik yang digunakan oleh penyerang *cyber* menyebabkan mereka tidak mampu mengidentifikasi tanda-tanda serangan yang umum terjadi, seperti *phishing*, *malware*, dan serangan virus. Hal ini berdampak pada keamanan data perusahaan dan meningkatkan risiko kebocoran data yang merugikan.

**2. Terjadinya Serangan Virus Tertentu yang Mengancam Keamanan Sistem Komputer Kapal**

Terjadinya serangan virus tertentu dapat mengancam keamanan sistem komputer kapal. Virus-virus ini menyusup ke dalam sistem komputer kapal melalui berbagai cara, seperti melalui email yang mengandung lampiran berbahaya atau melalui tautan yang merugikan.

Penyebabnya adalah :

**a. Tindakan Pengguna yang Tidak Aman**

Tindakan pengguna yang tidak aman dapat berkontribusi pada terjadinya serangan virus yang mengancam keamanan sistem komputer kapal. Contohnya, mengklik tautan atau membuka lampiran dari email yang mencurigakan atau tidak dikenal dapat memungkinkan virus masuk ke dalam sistem. Pengguna juga rentan terhadap serangan virus jika mereka mengunduh dan menginstal perangkat lunak dari sumber yang tidak terpercaya atau menggunakan perangkat lunak bajakan. Selain itu, menggunakan kata sandi yang lemah memberikan celah bagi penyerang

untuk meretas sistem.

Berikut ini adalah tabel yang menjelaskan dampak dari tindakan pengguna yang tidak aman terhadap terhadap keamanan sistem komputer kapal:

Tabel 3.2. Tindakan Pengguna yang Tidak Aman

| **Tindakan Pengguna yang Tidak Aman** | **Dampak Terhadap Keamanan Sistem Komputer Kapal** |
|---|---|
| Membuka email dari sumber yang tidak dikenal atau mencurigakan | Virus masuk ke dalam sistem melalui tautan atau lampiran yang berbahaya |
| Mengunduh dan menginstal perangkat lunak dari sumber yang tidak terpercaya | Virus atau perangkat lunak berbahaya lainnya untuk menginfeksi sistem |
| Menggunakan kata sandi yang lemah atau mudah ditebak | Meningkatkan risiko peretasan sistem dan akses tidak sah oleh pihak yang tidak berwenang |
| Membagikan informasi pribadi secara tidak aman | Menyediakan celah bagi penyerang untuk melakukan serangan phishing atau mencuri identitas |
| Mengklik tautan yang mencurigakan atau tidak diketahui | Mengarahkan pengguna ke situs web yang berbahaya yang dapat menyebabkan infeksi virus |
| Mengabaikan atau tidak menginstal pembaruan keamanan sistem | Meninggalkan kerentanan yang dapat dimanfaatkan oleh penyerang untuk meretas sistem |
| Menggunakan perangkat lunak bajakan | Meningkatkan risiko mendapatkan perangkat lunak yang telah dimodifikasi dan berpotensi berbahaya |

| Tindakan Pengguna yang Tidak Aman | Dampak Terhadap Keamanan Sistem Komputer Kapal |
|---|---|
| Tidak melakukan pencadangan data secara teratur | Meningkatkan risiko kehilangan data penting akibat serangan virus atau kerusakan sistem |

**b. Kurangnya Kesadaran akan Dampak Serangan Virus**

Kurangnya kesadaran akan dampak serangan virus menyebabkan ancaman terhadap keamanan sistem komputer kapal. Beberapa fakta adalah sebagai berikut:

1) Serangan virus menyebabkan kehilangan data yang berharga, seperti informasi pelanggan, dokumen penting, atau catatan operasional. Hal ini dapat mengganggu operasi kapal.

2) Serangan virus yang tidak terkendali menyebar ke jaringan lain yang terhubung dengan sistem komputer kapal, termasuk jaringan perusahaan atau mitra bisnis. Ini mengakibatkan penyebaran virus yang lebih luas dan menyebabkan kerugian yang lebih besar.

Hanya MV. EVER OCEAN yang mengalami masalah dampak serangan *cyber security*. Dalam kasus ini, serangan siber menyebabkan gangguan pada operasi dan keamanan kapal tersebut. Kasus serangan *cyber security* pada MV. EVER OCEAN adalah pengingat penting bahwa ancaman *cyber security* dapat terjadi pada semua sektor, termasuk industri pelayaran. Oleh karena itu, perusahaan harus selalu waspada terhadap ancaman ini dan mengambil langkah-langkah yang diperlukan untuk melindungi sistem dan data dari serangan yang terjadi.

## C. PEMECAHAN MASALAH

### 1. Alternatif Pemecahan Masalah

**a. Kurangnya Pemahaman *Crew* Terhadap *Cyber Security* di Atas Kapal Berdampak Bocornya Data-Data Perusahaan**

Alternatif pemecahannya adalah sebagai berikut :

**1) Melakukan pelatihan dan pendidikan yang lebih intensif kepada kru kapal mengenai prosedur penerapan *cyber security***

Bagi awak kapal, terkait dengan keamanan siber atau *cyber security*, pelatihan dan pendidikan sangat penting untuk melindungi sistem informasi dan teknologi yang digunakan dalam operasi kapal. Berikut beberapa jenis pelatihan dan pendidikan yang dapat relevan untuk awak kapal terkait dengan *cyber security*:

a) Pelatihan Kesadaran Keamanan *Cyber* (*Cyber Security Awareness Training*)

Pelatihan dasar yang bertujuan untuk meningkatkan kesadaran awak kapal tentang risiko *cyber security*, seperti serangan *phishing*, *malware*, dan praktik keamanan dasar.

b) Pelatihan Penanganan Insiden Keamanan (*Security Incident Handling Training*)

Pelatihan ini mengajarkan awak kapal bagaimana mengenali, mengatasi, dan merespons insiden *cyber security* dengan benar, termasuk langkah-langkah untuk menghentikan serangan dan memulihkan sistem.

c) Pelatihan Kepatuhan Regulasi Keamanan (*Security Regulation Compliance Training*)

Pelatihan ini akan membantu awak kapal memahami peraturan *cyber security* yang berlaku dalam industri pelayaran dan bagaimana mematuhi standar tersebut.

Tujuan konkret dari melakukan pelatihan dan pendidikan yang lebih intensif kepada awak kapal mengenai prosedur penerapan keamanan *cyber* adalah untuk meningkatkan pemahaman mereka tentang konsep dasar dan praktik terkait dengan keamanan *cyber*. Berikut ini adalah beberapa tujuan yang ingin dicapai melalui pelatihan dan pendidikan yang lebih intensif:

Salah satu tujuan utama dari pelatihan ini adalah untuk memastikan bahwa awak kapal memahami berbagai ancaman

keamanan *cyber* yang mungkin dihadapi kapal. Mereka akan belajar tentang jenis serangan yang umum, seperti serangan malware, serangan phishing dan serangan ransomware. Dengan pemahaman yang lebih baik tentang ancaman ini, kru kapal akan dapat mengidentifikasi dan merespons serangan dengan lebih efektif.

Pelatihan yang lebih intensif akan membantu awak kapal untuk mengenali tanda-tanda serangan *cyber* yang sedang terjadi. Mereka akan mempelajari indikator serangan, seperti perubahan yang mencurigakan dalam perilaku sistem, aktivitas jaringan yang tidak biasa, atau adanya upaya yang berulang untuk mendapatkan informasi sensitif. Dengan mengenali tanda-tanda ini, awak kapal dapat mengambil tindakan pencegahan yang diperlukan untuk menghentikan serangan sebelum merusak sistem.

Pelatihan akan mencakup pemahaman tentang prinsip dasar keamanan *cyber*, seperti prinsip kebutuhan untuk tahu (*need to know*), prinsip keberlanjutan bisnis (*business continuity*), dan prinsip pertahanan dalam kedalaman (*defense in depth*). Awak kapal belajar tentang pentingnya mengelola hak akses, melakukan pemantauan jaringan secara teratur, dan menjaga kepatuhan terhadap kebijakan keamanan. Pemahaman yang mendalam tentang prinsip-prinsip ini akan membantu awak kapal dalam mengambil langkah-langkah yang tepat untuk melindungi sistem kapal dari serangan *cyber*.

Tujuan lain dari pelatihan ini adalah untuk mengajarkan kru kapal tentang langkah-langkah keamanan yang harus diimplementasikan untuk melindungi sistem kapal. Mereka akan belajar tentang kebutuhan untuk memiliki perangkat lunak keamanan yang terbaru dan diperbarui, mengamankan jaringan dengan *firewall* dan enkripsi, serta menerapkan kebijakan kata sandi yang kuat dan penggunaan autentikasi dua faktor. Dengan memahami langkah-langkah ini, awak kapal dapat mengimplementasikan praktik keamanan yang tepat untuk

melindungi sistem dari serangan cyber.

Pelatihan yang lebih intensif akan melibatkan simulasi serangan *cyber* dan latihan respons terhadap serangan tersebut. Awak kapal akan belajar tentang langkah-langkah yang harus diambil dalam merespons serangan, termasuk penghentian serangan, mitigasi kerusakan, dan pemulihan sistem. Latihan ini akan membantu awak kapal untuk memperoleh keterampilan dan pengetahuan yang diperlukan dalam menghadapi serangan *cyber* dengan cepat dan efektif.

**2) Memperkuat kebijakan dan prosedur *cyber security* di kapal**

Memperkuat kebijakan dan prosedur *cyber security* di kapal merupakan langkah penting dalam mengatasi kurangnya pemahaman awak kapal terhadap *cyber security*. Peraturan manajemen tentang perangkat penyimpanan massal USB di atas kapal armada diterapkan di dalam armada perusahaan dengan memastikan bahwa setiap kapal dan awak kapal mematuhi persyaratan yang telah ditetapkan. Peraturan ini seperti pada langkah 5 dan 6 akan dimasukkan ke dalam agenda Rapat Bulanan Kapal setiap bulannya .

Berikut adalah tabel yang penjelasan mengenai langkah-langkah yang dilakukan untuk menghilangkan *cyber-risk* pada perangkat USB:

Tabel 3.3. Langkah-Langkah Menghilangkan *Cyber-Risk* USB

| Langkah-langkah | Penjelasan |
|---|---|
| 1. Pembatasan penggunaan USB | Mengatur kebijakan yang membatasi atau mengatur penggunaan perangkat USB di kapal. Hal ini dapat dilakukan dengan membatasi akses fisik terhadap port USB, menggunakan perangkat lunak yang mengontrol akses ke perangkat USB, atau menerapkan kebijakan yang mengharuskan penggunaan perangkat USB hanya |

| Langkah-langkah | Penjelasan |
|---|---|
| | melalui prosedur yang ditetapkan secara resmi. |
| 2. Penggunaan perangkat lunak | Menginstal perangkat lunak keamanan yang memantau dan melindungi sistem komputer dari ancaman yang berasal dari perangkat USB. Perangkat lunak ini harus mampu mendeteksi dan menghapus *malware* yang terkait dengan perangkat USB, serta memberikan laporan atau peringatan jika ada aktivitas mencurigakan terkait dengan penggunaan perangkat USB. |
| 3. Pemindaian perangkat USB | Melakukan pemindaian terhadap perangkat USB sebelum digunakan di komputer kapal. Pemindaian ini akan membantu mendeteksi adanya *malware* atau file yang mencurigakan pada perangkat USB sebelum dapat menyebar ke sistem komputer kapal. |
| 4. Pemutakhiran perangkat lunak | Memastikan bahwa semua perangkat lunak yang digunakan di sistem komputer kapal, termasuk perangkat lunak keamanan, selalu diperbarui dengan versi terbaru. Pemutakhiran ini penting untuk mengatasi kerentanan keamanan yang dapat dieksploitasi oleh *malware* yang menyebar melalui perangkat USB. |
| 5. Pemantauan dan pelaporan | Melakukan pemantauan terhadap aktivitas penggunaan perangkat USB |

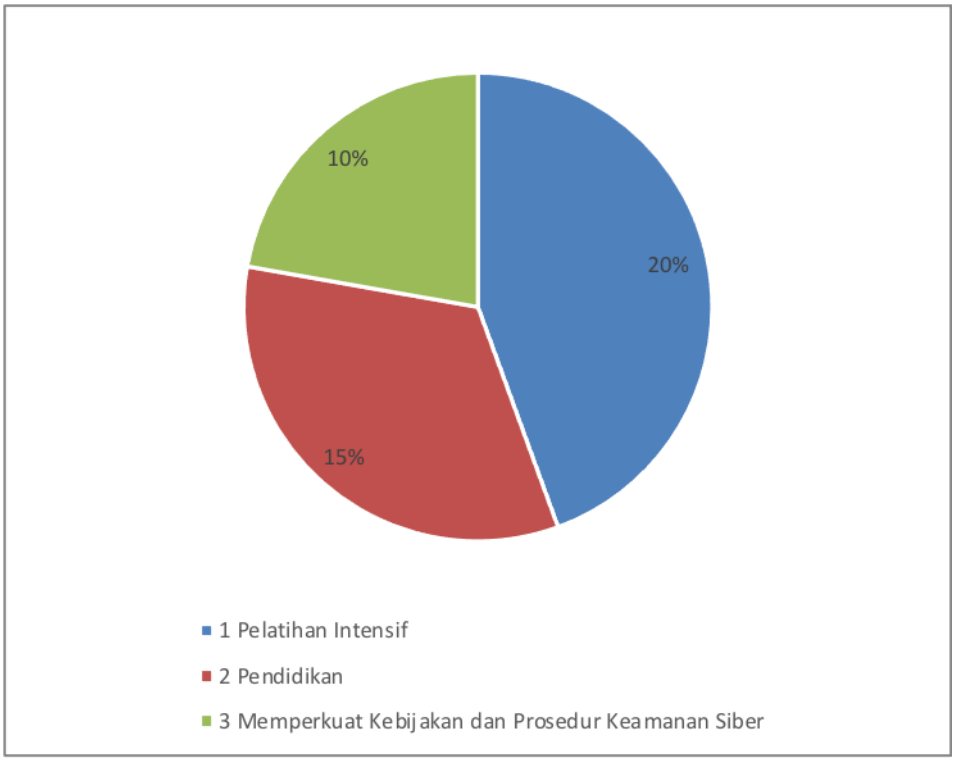
| Langkah-langkah | Penjelasan |
|---|---|
| | di kapal. Hal ini dapat dilakukan dengan menggunakan perangkat lunak pemantauan jaringan atau log aktivitas sistem. Selain itu, pelaporan terkait dengan penggunaan perangkat USB yang melanggar kebijakan atau mencurigakan dapat membantu dalam mengidentifikasi dan mengatasi ancaman keamanan secepat mungkin. |
| 6. Tindakan disipliner | Menetapkan sanksi atau tindakan disipliner yang tegas terhadap awak kapal yang melanggar kebijakan penggunaan perangkat USB. Tindakan ini dapat mencakup teguran, denda, atau bahkan pemecatan jika pelanggaran tersebut dianggap serius dan mengancam keamanan sistem komputer kapal. |

Berikut adalah tabel dalam persentase yang menunjukkan bahwa setelah melakukan pelatihan dan pendidikan yang lebih intensif kepada kru kapal mengenai prosedur penerapan keamanan siber, serta memperkuat kebijakan dan prosedur keamanan siber di kapal, dampak bocornya data-data perusahaan mengalami penurunan pada tahun 2021.

Tabel 3.4. Tingkat dampak yang lebih rendah setelah tindakan yang diambil tahun 2021

| No. | Tindakan yang Dilakukan | Persentase Dampak Bocornya Data |
|---|---|---|
| 1 | Pelatihan Intensif | 20% |
| 2 | Pendidikan | 15% |
| 3 | Memperkuat Kebijakan dan Prosedur Keamanan Siber | 10% |

Dalam gambar diagram lingkaran dibawah ini, angka persentase digunakan untuk menggambarkan tingkat dampak yang lebih rendah setelah tindakan yang diambil pada tahun 2021.



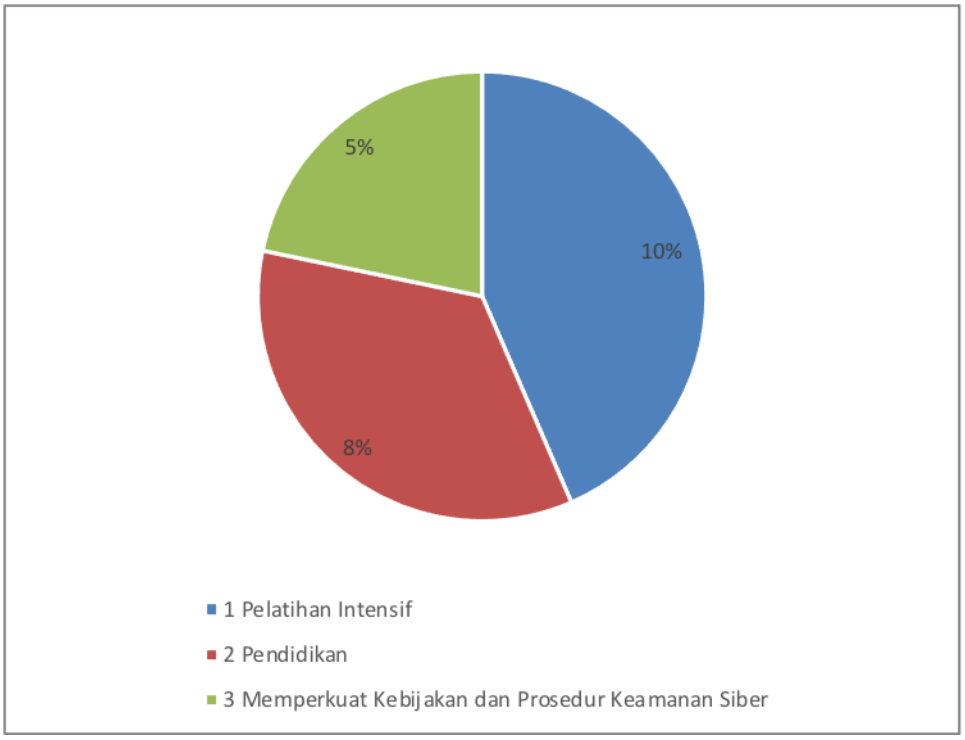

Gambar 3.1. Diagram lingkaran tahun 2021

Berikut adalah tabel dalam persentase yang menunjukkan bahwa setelah melakukan pelatihan dan pendidikan yang lebih intensif kepada kru kapal mengenai prosedur penerapan keamanan siber, serta memperkuat kebijakan dan prosedur keamanan siber di kapal, dampak bocornya data-data perusahaan mengalami penurunan pada tahun 2022.

Tabel 3.5. Tingkat dampak yang lebih rendah setelah tindakan yang diambil tahun 2022

| No. | Tindakan yang Dilakukan | Persentase Dampak Bocornya Data |
|---|---|---|
| 1 | Pelatihan Intensif | 10% |
| 2 | Pendidikan | 8% |
| 3 | Memperkuat Kebijakan dan Prosedur Keamanan Siber | 5% |

Dalam gambar diagram lingkaran dibawah ini, angka persentase digunakan untuk menggambarkan tingkat dampak yang lebih rendah setelah tindakan yang diambil pada tahun 2022.




Gambar 3.2. Diagram lingkaran tahun 2022

**b. Terjadinya Serangan Virus Tertentu yang Mengancam Keamanan Sistem Komputer Kapal**

Alternatif pemecahannya adalah sebagai berikut :

**1) Menggunakan perangkat lunak keamanan yang mutakhir dan pembaruan sistem**

Menggunakan perangkat lunak keamanan yang mutakhir dan pembaruan sistem adalah langkah penting dalam menjaga keamanan sistem komputer kapal dari serangan virus yang mengancam. Serangan virus tertentu menyebabkan kerusakan serius pada sistem komputer kapal, mengakibatkan gangguan operasional, dan kebocoran data sensitif. Perusahaan seperti *Microsoft*, secara rutin merilis pembaruan keamanan untuk sistem operasi guna memperbaiki kerentanan yang ditemukan.

Perangkat lunak keamanan yang mutakhir merujuk pada

*software* yang dirancang khusus untuk mendeteksi, mencegah, dan menghapus ancaman *malware*, termasuk serangan virus. Jenis perangkat lunak keamanan yang umum digunakan termasuk anti virus selain *Symantec Endpoint*, *Windows Defender Firewall* (bawaan dalam sistem operasi *Windows*), dan *antispyware Windows Defender* (bawaan dalam sistem operasi *Windows*). Anti virus digunakan untuk mendeteksi dan menghapus virus yang ada dalam sistem, sementara *firewall* bertindak sebagai penghalang untuk melindungi sistem dari serangan jaringan yang tidak sah. *Antispyware* berfungsi untuk mendeteksi dan menghapus perangkat lunak mata-mata yang mencoba mengakses informasi sensitif.

Selain menggunakan perangkat lunak keamanan yang mutakhir, penting juga untuk secara rutin melakukan pembaruan sistem. Pembaruan sistem termasuk menginstal *patch* keamanan terbaru dan memperbarui versi perangkat lunak yang digunakan. Pembaruan sistem penting karena seringkali vendor perangkat lunak merilis pembaruan untuk memperbaiki kerentanan keamanan yang ditemukan. Dengan memperbarui sistem secara rutin, memastikan bahwa kelemahan yang diketahui telah diperbaiki dan sistem komputer kapal dan jaringan tanpa kabel atau *wireless network security* tetap aman dari serangan virus tertentu.

**2) Menerapkan kebijakan penggunaan perangkat pribadi**

Terjadinya serangan virus tertentu yang mengancam keamanan sistem komputer kapal, menerapkan kebijakan penggunaan perangkat pribadi menjadi sangat penting. Keamanan sistem komputer kapal sangatlah krusial, mengingat kapal memiliki sistem yang kompleks dan ketergantungan yang tinggi terhadap teknologi komputer.

Perangkat yang tersambung ke komputer adalah USB yang mencakup semua perangkat yang menggunakan port standar USB MSC dan terhubung ke komputer, termasuk *hard drive* eksternal (termasuk *solid-state drive*), *drive* optik eksternal (termasuk *drive* pembaca/penulis CD dan DVD), perangkat memori *flash* portabel,

kamera digital, audio digital dan pemutar media *portabel*, pembaca kartu, PDA, pengontrol antarmuka jaringan nirkabel, dan ponsel cerdas.

Dalam Surat Edaran Kelautan Evergreen Grup yang disebutkan, "Dua Praktik Terbaik untuk menghilangkan *cyber-risk* pada perangkat USB" ditekankan sebagai langkah-langkah yang harus diikuti untuk mengurangi *cyber-risk* yang terkait dengan penggunaan perangkat USB. Berikut adalah penjelasan mengenai dua praktik terbaik tersebut:

a) Batasi penggunaan perangkat USB eksternal

Praktik pertama yang direkomendasikan adalah membatasi penggunaan perangkat USB eksternal. Hal ini dimaksudkan untuk mengurangi infeksi virus atau *malware* yang dapat terjadi melalui perangkat USB yang tidak dikenal. Beberapa langkah yang dapat diambil dalam implementasi praktik ini antara lain:

(1) Batasi penggunaan perangkat USB dari sumber yang dapat dipercaya

Disarankan untuk hanya menggunakan perangkat USB yang berasal dari sumber yang terpercaya dan dijamin bebas dari virus atau *malware*. Perangkat USB yang diperoleh dari sumber yang tidak diketahui atau tidak dapat dipercaya memiliki risiko yang lebih tinggi untuk mengandung ancaman *cyber*.

(2) Gunakan perangkat USB yang telah diverifikasi keamanannya

Selalu pastikan bahwa perangkat USB yang digunakan telah diverifikasi keamanannya. Beberapa perusahaan menyediakan perangkat USB yang telah diuji dan disertifikasi bebas dari ancaman *cyber*. Penggunaan perangkat USB yang telah diverifikasi dapat membantu mengurangi risiko serangan *cyber*.

(3) Implementasikan kebijakan penggunaan perangkat USB

Organisasi dapat mengimplementasikan kebijakan yang mengatur penggunaan perangkat USB di tempat kerja. Kebijakan ini dapat mencakup aturan tentang penggunaan perangkat USB eksternal, prosedur pemeriksaan keamanan, dan langkah-langkah mitigasi risiko yang harus diikuti oleh karyawan.

b) Periksa dan *scan* perangkat USB sebelum digunakan

Praktik kedua yang direkomendasikan adalah memeriksa dan memindai perangkat USB sebelum digunakan. Tujuannya adalah untuk mendeteksi dan menghapus potensi ancaman *cyber* sebelum perangkat USB tersebut digunakan di sistem yang rentan. Beberapa langkah yang dapat diambil dalam implementasi praktik ini antara lain:

(1) Gunakan perangkat lunak keamanan yang terpercaya

Pastikan perangkat lunak keamanan yang digunakan untuk memeriksa dan memindai perangkat USB adalah yang terpercaya dan diperbarui secara teratur. Perangkat lunak anti virus dan anti-*malware* yang handal membantu mendeteksi dan menghapus ancaman *cyber* yang ada di perangkat USB.

(2) Lakukan pemeriksaan dan pemindaian secara berkala

Disarankan untuk secara rutin melakukan pemeriksaan dan pemindaian perangkat USB sebelum digunakan di sistem yang rentan. Dengan melakukan ini secara teratur, potensi ancaman *cyber* dapat dideteksi lebih awal dan tindakan pencegahan yang tepat dapat diambil.

(3) Perbarui definisi dan tanda tangan keamanan

Pastikan perangkat lunak keamanan yang digunakan diperbarui dengan definisi dan tanda tangan terbaru. Hal ini penting untuk memastikan bahwa perangkat lunak dapat mengenali dan melawan ancaman *cyber* terbaru yang ada di

perangkat USB.

Dengan menerapkan kedua praktik terbaik ini, diharapkan *cyber-risk* yang terkait dengan penggunaan perangkat USB dapat dikurangi secara signifikan. Penting bagi semua pihak terkait untuk mematuhi dan mengikuti langkah-langkah ini demi keamanan informasi dan sistem yang lebih baik.

**2. Evaluasi Terhadap Alternatif Pemecahan Masalah**

**a. Kurangnya Pemahaman *Crew* Terhadap *Cyber Security* di Atas Kapal Berdampak Bocornya Data-Data Perusahaan**

**1) Melakukan pelatihan dan pendidikan yang lebih intensif kepada *crew* kapal mengenai prosedur penerapan *cyber security***

a) Keuntungannya :

(1) Dengan melakukan pelatihan dan pendidikan yang lebih intensif kepada *crew* kapal mengenai prosedur penerapan *cyber security*, akan meningkatkan kesadaran terhadap ancaman *cyber* dan pentingnya melindungi data dan sistem kapal dari serangan *cyber*.

(2) *Crew* kapal akan mendapatkan pengetahuan dan keterampilan yang ditingkatkan dalam melaksanakan prosedur penerapan *cyber security*. Mereka akan memahami lebih baik tentang praktek terbaik dan tindakan yang harus diambil untuk mengurangi *cyber-risk*..

b) Kerugiannya :

(1) Pelatihan dan pendidikan intensif membutuhkan biaya dan waktu yang lebih. Perusahaan harus mengalokasikan anggaran dan sumber daya untuk melaksanakan program pelatihan tersebut, serta mengatur jadwal agar *crew* kapal dapat mengikuti pelatihan tanpa mengganggu operasional kapal.

(2) Meskipun pelatihan dan pendidikan intensif dilakukan, masih ada potensi ketidakkonsistenan dalam penerapan prosedur

*cyber security* di antara *crew* kapal. Setiap individu memiliki tingkat pemahaman dan kepatuhan yang berbeda-beda, sehingga masih mungkin ada kesalahan atau kelalaian dalam melaksanakan prosedur yang dapat meningkatkan *cyber-risk*.

**2) Memperkuat kebijakan dan prosedur *cyber security* di kapal**

a) Keuntungannya :

(1) Memperkuat kebijakan dan prosedur *cyber security*, kapal dapat mengurangi risiko serangan *cyber* yang dapat menyebabkan kerusakan sistem, pencurian data, atau gangguan pada operasi kapal. Ini membantu melindungi integritas dan kerahasiaan informasi penting.

(2) Mengedepankan kebijakan dan prosedur yang kuat, awak kapal lebih sadar ancaman *cyber security* dan pentingnya penerapan tindakan pencegahan yang tepat. Hal ini mengurangi kesalahan manusia dan meningkatkan kepatuhan terhadap kebijakan *cyber security*.

b) Kerugiannya :

(1) Memperkuat kebijakan dan prosedur *cyber security* di kapal membutuhkan waktu dan sumber daya yang cukup. Ini melibatkan pelatihan awak kapal, penerapan infrastruktur keamanan yang memadai, dan pemantauan yang berkelanjutan. Hal ini menimbulkan biaya tambahan dan membutuhkan komitmen yang kuat dari perusahaan.

(2) Implementasi kebijakan dan prosedur *cyber security* yang ketat dapat mengakibatkan pembatasan atau peningkatan langkah-langkah keamanan yang mempengaruhi efisiensi operasional kapal. Misalnya, penggunaan sistem keamanan yang kuat mengharuskan proses otentikasi yang lebih rumit, yang memakan waktu lebih lama dan mengurangi produktivitas awak kapal.

**b. Terjadinya Serangan Virus Tertentu yang Mengancam Keamanan**

**Sistem Komputer Kapal**

**1) Menggunakan perangkat lunak keamanan yang mutakhir dan pembaruan sistem**

a) Keuntungannya :

(1) Perangkat lunak keamanan yang mutakhir dapat mendeteksi dan mengatasi ancaman keamanan yang lebih baru dan kompleks dengan lebih efektif, memberikan perlindungan yang lebih baik untuk sistem.

(2) Perangkat lunak keamanan yang mutakhir dapat memberikan pemantauan *real-time* terhadap aktivitas jaringan dan sistem, sehingga memungkinkan deteksi dini dan penanggulangan cepat terhadap serangan yang terjadi.

b) Kerugiannya :

(1) Perangkat lunak keamanan yang mutakhir umumnya memiliki biaya yang lebih tinggi dibandingkan dengan solusi keamanan yang lebih sederhana atau yang sudah usang.

(2) Perangkat lunak keamanan yang mutakhir biasanya membutuhkan sumber daya sistem yang lebih besar, seperti daya pemrosesan dan ruang penyimpanan.

**2) Menerapkan kebijakan penggunaan perangkat pribadi**

a) Keuntungannya :

(1) Kebijakan penggunaan perangkat pribadi, perusahaan dapat mengendalikan akses dan perlindungan terhadap data sensitif. Dengan membatasi penggunaan perangkat pribadi, risiko kebocoran data atau akses yang tidak sah dapat dikurangi. Perusahaan dapat menerapkan langkah-langkah keamanan tambahan pada perangkat yang diizinkan untuk digunakan, seperti enkripsi data atau penghapusan jarak jauh jika perangkat hilang.

(2) Kebijakan penggunaan perangkat pribadi memungkinkan *crew* untuk bekerja menggunakan perangkat yang mereka pilih dan nyaman dengan mereka. Ini meningkatkan produktivitas karena *crew* dapat menggunakan perangkat yang mereka kuasai dengan baik dan yang cocok dengan kerja mereka. Mereka dapat mengakses informasi dan alat kerja mereka dengan mudah di perangkat pribadi mereka, yang dapat meningkatkan efisiensi kerja.

b) Kerugiannya :

(1) Mengizinkan penggunaan perangkat pribadi meningkatkan risiko keamanan IT. Perangkat pribadi tidak memiliki langkah-langkah keamanan yang sama dengan perangkat yang disediakan oleh perusahaan. Ini dapat membuka celah keamanan yang dapat dimanfaatkan oleh penyerang untuk mengakses sistem atau data perusahaan. Perusahaan harus mengimplementasikan kebijakan yang ketat dan mengharuskan perangkat pribadi untuk memenuhi standar keamanan tertentu.

(2) Mengelola berbagai jenis perangkat pribadi yang berbeda dapat menjadi tugas yang rumit. Perusahaan perlu mempertimbangkan kompatibilitas perangkat, pembaruan sistem operasi, dan perangkat lunak yang berbeda. Ini dapat meningkatkan kompleksitas pengelolaan IT dan memerlukan sumber daya tambahan untuk menjaga perangkat pribadi tetap aman, terkini, dan sesuai dengan kebijakan perusahaan.

**3. Pemecahan Masalah yang Dipilih**

**a. Kurangnya Pemahaman *Crew* Terhadap *Cyber Security* di Atas Kapal Berdampak Bocornya Data-Data Perusahaan**

Berdasarkan evaluasi terhadap alternatif pemecahan masalah di atas, maka solusi yang dipilih untuk mengatasinya yaitu dengan melakukan pelatihan dan pendidikan yang lebih intensif kepada *crew* kapal mengenai prosedur penerapan *cyber security*.

**b. Terjadinya Serangan Virus Tertentu yang Mengancam Keamanan Sistem Komputer Kapal**

Berdasarkan evaluasi terhadap alternatif pemecahan masalah di atas, maka solusi yang dipilih untuk mengatasinya yaitu dengan menggunakan perangkat lunak keamanan yang mutakhir dan pembaruan sistem.

# BAB IV
# KESIMPULAN DAN SARAN

## A. KESIMPULAN

Berdasarkan bab sebelumnya yang telah disampaikan, maka penulis menyimpulkan sebagai berikut:

1. Kurangnya pemahaman terhadap *cyber security* diatas kapal berdampak pada bocornya data-data perusahaan disebabkan oleh kurangnya pahaman anak buah kapal.
2. Terjadinya serangan virus tertentu yang mengancam keamanan sistem komputer kapal dapat diatasi dengan penggunaan peralatan / perangkat lunak keamanan mutakhir dan pembaharuan sistem.

## B. SARAN

Dari uraian pada kesimpulan di atas, Penulis memberikan saran-saran sebagai berikut:

1. Kepada perusahaan:
    a. Mengintensifkan pendidikan tentang praktik keamanan *cyber* kepada *crew* kapal, termasuk pentingnya prosedur penerapan *cyber security* dan strategi dalam melindungi sistem komputer kapal.
    b. Menyusun prosedur yang jelas mengenai pembaruan sistem, termasuk langkah-langkah yang harus diambil untuk memeriksa, menginstal, dan memverifikasi pembaruan yang diperlukan.
    c. Perusahaan harus memiliki mekanisme pemantauan dan pelaporan insiden keamanan. *Crew* harus diberi tahu untuk segera melaporkan setiap kejadian mencurigakan atau pelanggaran keamanan yang mereka temui.

2. Kepada nakhoda/perwira kapal:

    a. Memastikan sistem operasi dan perangkat lunak yang digunakan di kapal selalu diperbarui ke versi terbaru mencakup perbaikan keamanan yang dapat melindungi sistem dari serangan virus dan ancaman lainnya.

    b. Memberikan pelatihan dan edukasi kepada seluruh *crew* kapal tentang pentingnya keamanan sistem komputer dan langkah-langkah yang harus diambil untuk mencegah serangan virus.

    c. Meninjau dan memperbarui kebijakan keamanan *cyber* kapal secara berkala dan memastikan kebijakan mencakup praktik keamanan *cyber* yang relevan terhadap penggunaan perangkat pribadi, persyaratan kata sandi yang kuat, dan kebijakan penggunaan internet.

# DAFTAR PUSTAKA


Arini T. Soemohadiwidjojo. (2014). *Mudah Menyusun Standard Operating Procedure (SOP)*. Perum Bukit Permai. Jakarta.

Asep Chaerudin, M.A.S.S. (2018). *Panduan Penanganan Insiden Malicious Software (Malware).* BSSN. Jakarta.

Eko Budi. (2021). *Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5*.0. Akademi Angkatan Udara. Yogyakarta

Elok Nuriyanto (2020). *Peningkatan Hasil Belajar Siswa Melalui Model Pembelajaran Kooperatif Tipe Two Stay Two Stray (TSTS).* Suluh Edukasi. Lombok.

Evergreen Marine Corporation. (2023). *Ship Particular dan data kapal*.

Koh, B. (t.t.): Richard A. Clarke and Robert K. Knake (2010). *Cyber War: The Next Threat to National Security and What to Do about It.* HarperCollins Publishers. New York.

M.A. Ibrahim. (2015). *Metode Penelitian Kualitatif* . Perpustakaan Nasional. Pontianak.

Obrina Candra Briliyant (2020). *Improving Security of Web-Based Application Using ModSecurity and Reverse Proxy in Web Application Firewall*. STSN. Jakarta.

Sari Eka Pratiwi. (2018). Pengaruh Pelatihan dan Disiplin Kerja Terhadap Kinerja Karyawan. Medan.

Sugiyono, 2010 *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. PT Alfabet. Bandung.

The Guidelines on Cyber Security Onboard Ships (2020).

Wahyu Tisno Atmojo (2021). *Pengenalan Cyber Security Dalam Revousi Industri Dan Menyongsong Era Society 5.0*. PKM-CSR. Banten.

Wang, F.-Y., Yuan, Y., Wang, X., & Qin, R. (2018*). Societies 5.0: A New Paradigm for Computational Social Systems Research*. IEEE. Ottawa.

Yuni Selvita Suci (2018). *Rancang Bangun Sistem Keamanan Data Komputer Pada Antivirus Vici Menggunakan Sistem Realtime Protector dan Metode Heuristic Ganda*. Politeknik Negeri Sriwijaya. Palembang.

# LAMPIRAN

## LAMPIRAN 1

船 舶 明 細 表

**PARTICULARS**

| | | | | | |
|---|---|---|---|---|---|
| 船 名 | Ship Name | EVER OCEAN 長洋 | 註 冊 港 | Port of Registry | Hong Kong |
| 船 東 | Buyer | Evergreen Marine (Hong Kong) Ltd. | 註 冊 編 號 | Official No. | HK-5474 |
| 國 籍 | Flag of Ship | Hong Kong | 呼 號 | Call Sign | VRTV9 |
| 船 型 | Type | Container carrier | 標 識 編 號 | MMSI No. | 477664500 |
| | | | 國際海事組織編號 | IMO No. | 9872389 |
| | | | 衛星通訊呼號 | Inmarsat Fleet FB500 | Voice 870773061089 |
| | | | | | Fax 870783899291 |
| 船 級 | Class / No. | NK / 210784 | | Inmarsat Glob. Xpress | Voice1 (65)31659957 |
| | Class Notation | NS * (CNC, EQ C DG, PSPC-WBT, NC) (PS-DA&FA)(IWS)(PSCM)(EA) (IHM)(CSSA-R) (SOx(EGCS) ), MNS* Installation Characters: CHG, M0, MPP, LSA, RCF, AFS, BWM | | | Voice2 (65)31659958 |
| | | | 衛星通訊呼號 | Tlx / Inmarsat C No. | 447766450 |
| | | | | | 447766451 |
| | | | 電 子 郵 件 | E-mail | master.EVEROCEAN@fleetmail.inmarsat.com |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 建 造 年 | Built Keel Laid | Aug. 07, 2020 | | 甲 板 | Deck Plan | 1 |
| | Launched | Nov. 24, 2020 | | 艙 壁 | Bulkhead | 8 |
| | Delivered | Apr. 26, 2021 | | 貨 艙 | Holds | 4 |
| 建 造 廠 | Builder | JIANGNAN shipyard(group) Co.,Ltd | | 艙 口 蓋 | Hatch Cover | 26 |
| 材 質 | Material | STEEL | | 吊 貨 機 | Provision Cranes | Monorail type / 7.0 MT x 1 set |
| 定 檢 | Special Survey | | | 吊桿/絞機 | Derricks / Winches | NIL / 8 |
| | | Designed | Registered | 主 機 | Main Engine Type | WinGD W8X62-B,LLT,Tier II |
| 總 長 | Length O.A. | 195.00 M | | 製 造 廠 | Engine Maker | CSSC-MES Diesel Co.,Ltd |
| 法 長 | Length B.P. | 191.80 M | 191.82 M(ITC) | 主機位置 | Engine Placed | Semi-Aft |
| 船 寬 | Breadth MLD. | 32.25 M | 32.25 M(ITC) | 馬力 x 轉數 | BHP x RPM SMCR | 15,000 kW x 90.0 RPM |
| 船 深 | Depth MLD. | 17.00 M | 17.00 M(ITC) | | NCR | 13,500 kW x 86.9 RPM |
| 設計吃水 | Designed Draft (Td) | 10.00 M | | 耗 油 量 | Oil Consump. of ME | 50.9 MT/Day (LCV 10,200Kcal/kg) |
| 寸法吃水 | Scantling Draft (Ts) | 11.20 M | 11.2 M(ITC) | | | at 90%DMCR |
| 總船高 | Air Draft | 52.1 M | | | Oil Consump. | |
| 總 噸 位 | Gross Tonnage | 29,116 | (ITC) | | of GE/set | 192 g/kWh at 100% output |
| 淨 噸 位 | Net Tonnage | 11,183 | (ITC) | | | |
| | | | | 艏 側 推 器 | Bow Thruster | NT-C070 |
| 載貨重量 | Deadweight (Td / Ts) | 26,756.1/32,830.9 MT | | | Bow Thruster Maker | NAKASHIMA |
| | | | | 馬力 x 轉數 | kW x RPM | 1,200 kW x 327.3 RPM x 1 set |
| 船 速 | Speed (Td) | 20.07 Knots at NCR (Trial Result) | | 輔助鍋爐 | Aux. Boiler Type | Vertical Water Tube Boiler |
| 貨櫃容積 | Container (on deck) | 1,712 TEU | (7 tiers) | | | MC-30D x 1 set |
| | Container (in hold) | 922 TEU | | 製 造 廠 | Boiler Maker | CSSC Jiujiang boiler Co.,Ltd. |
| | Total | 2,634 TEU | | 工作壓力 | Working Pressure | 7.0 kg/cm$^2$ |
| 冷櫃插座 | Ref. Container (deck) | 226 Plug | | 發 電 機 | Generator Engine | 6DK-26e x 3 sets |
| | Ref. Container (hold) | Nil | | 製 造 廠 | Generator Eng. Maker | Anqing CSSC diesel engine Co.,Ltd |
| | Total | 226 Plug (Powered 226 Plug) | | | Generator Maker | Zhenjiang China marine xiandai gen. Co.,Ltd |
| | Stack load (20ft / 40ft) | 80 MT/140 MT on Hatch | | 發 電 量 | Generator Capacity | 1,400 kW / 60 Hz / AC 450V |
| | Stack load (20ft / 40ft) | 30.48 MT/30.48MT in hold /tier | | 緊急發電機 | Emergency Generator | 220 kW / 60 Hz / AC 450V |
| 燃 油 量 | Capacity Fuel Oil "HFO" | abt. 1,600 CUB.M | | | | |
| | Capacity Fuel Oil "MGO" | abt. 400 CUB.M | | 航海儀器, | Nav. Equipment, | ECDIS, MC, RADAR, DGPS, AIS, |
| | Capacity "very low sulphur" | abt. 200 CUB.M | | 無線電及 | Radio and Special | VDR, ES, SL, AP, NAVTEX, VHF, |
| 淡 水 量 | Capacity Fresh Water | abt. 250 CUB.M | | 特別設備 | Equipments | MF/ HF radio JSS-2500, INM-C, |
| (飲水量) | (Drinking Water only) | abt. 60 CUB.M | | | | INM-FB500, SSAS, EPIRB, |
| 壓 水 艙 | Capacity Ballast Water | abt.12,400 CUB.M | | | | Weather facsimile receiver, GMDSS, |
| 壓艙水系統 | Ballast Pump | 500 CUB.M/H x 2 | | | | Rudder angle indicator |
| | Ballast Treatment System | 500 CUB.M/H x 1 | | 脫硫器 | Sox Scrubber | Open Loop U Type System |
| 巴拿馬噸位 | Panama Tonnage | 24,180 | | 防傾系統 | Anti-heeling System | 700 CBM/H x 1 set |

| | | | | | |
|---|---|---|---|---|---|
| | (PC/UMS Net Tonnage) | | 艙 口 蓋 | Hatch Cover Sizes: | Hatch Way Sizes: ( L x W ) |
| 蘇伊士噸位 | Suez Tonnage | G/T 30,592.62 | | Typical 12.810 x 10.370 (p/s) | 12.600 x 28.000 (nominal) |
| | | N/T 24,569.54 | | 12.805 x 7.500 (c) | |
| | | | | (Provisional) | (Apr. 08, 2021 Updated) |

# LAMPIRAN 2

GRT / NRT: 29,116 / 11,183
TYPE: CONTAINER VESSEL
CALL SIGN: VRTV9
FLAG: Hong Kong
LOCATION:
PIC:
TEL:

Regulation 31 (1)

**FORM 22**
**IMMIGRATION ACT**
**(CHAPTER 133)**

## IMMIGRATIONS REGULATIONS

## CREW LIST

*Name of Vessel: **EVER OCEAN** Owner: **Evergreen Marine (Hong Kong) Ltd.**

Agents in Singapore: **Evergreen Marine (Singapore) Pte Ltd.** Gross Tonage of Vessel: **29.116**

Last place of embarkation: **LAEM CHABANG (THAILAND)** Date of arrival: **12/Jul/2023**

Next destination: **TANJUNG PELEPAS(MALAYSIA)** Date of proposed departure: **13/Jul/2023**

| No. | Name | Sex | Date of Birth | Nationality | Travel Document No. | Expiry Date of Travel Document | Duties onboard |
|---|---|---|---|---|---|---|---|
| 1 | CHEN,XIAOXIANG | M | 26/Apr/1984 | CHINESE | EE3750516 | 13/Sep/2028 | MS |
| 2 | SULAKSONO,MUDA | M | 12/Jan/1971 | INDONESIA | X1250053 | 02/Dec/2026 | CO |
| 3 | HUTAURUK,OVER GRAND | M | 21/May/1992 | INDONESIA | E0791099 | 18/Nov/2032 | 2O |
| 4 | KATUUK,ANGELO REINALDY | M | 14/Jun/1972 | INDONESIA | C8675929 | 16/Mar/2027 | 3/O |
| 5 | ACUEZA,JUANN MIGUEL BARCENAS | M | 25/Aug/1998 | FILIPINO | P5744689B | 06/Nov/2030 | 3/O |
| 6 | ELLOSO,LORENZO VELUZ | M | 10/Aug/1962 | FILIPINO | P6772235A | 12/Apr/2028 | C/E |
| 7 | JARDIN,JOEMAR SALAYO | M | 03/Dec/1980 | FILIPINO | P4429277B | 16/Jan/2030 | 2E |
| 8 | MAJID,MAZHAR ABDUL | M | 13/Apr/1994 | INDONESIA | E3517647 | 12/May/2033 | 3E |
| 9 | EXTRADA,DELA IRLADE | M | 20/Apr/1989 | INDONESIA | C7404846 | 18/Feb/2026 | 4E |
| 10 | ARIFIN,HUSNUL | M | 08/Nov/1975 | INDONESIA | C9077702 | 30/May/2027 | BSN |
| 11 | PURNOMO | M | 04/Nov/1971 | INDONESIA | C7388314 | 19/Nov/2025 | AB |
| 12 | MAHMUDI | M | 03/Nov/1978 | INDONESIA | C8103495 | 24/Nov/2026 | AB |
| 13 | BINONI,HANS | M | 16/Sep/1989 | INDONESIA | C7167696 | 25/Jun/2025 | AB |
| 14 | ANAM,MUCH SHAEFUL | M | 17/May/1984 | INDONESIA | C8539450 | 16/Mar/2027 | AB |
| 15 | HARIS,ABDUL | M | 29/Dec/1983 | INDONESIA | E0791793 | 01/Dec/2032 | AB |
| 16 | MANGAHAS,ROMUALDO MARTIN | M | 07/Feb/1976 | FILIPINO | P9767321A | 29/Nov/2028 | FT |
| 17 | AGUILAR,KENNETH JONH FERNANDEZ | M | 15/Jun/1980 | FILIPINO | P6301993A | 05/Mar/2028 | MM |
| 18 | PERUCHO,ROLAND BINAS | M | 02/Oct/1973 | FILIPINO | P1489955B | 16/Apr/2029 | MM |
| 19 | WANG,JIN | M | 08/Jun/1969 | CHINESE | EE5718087 | 22/Oct/2028 | CCK |
| 20 | WANG,YONG | M | 29/Jun/1999 | CHINESE | EJ5891564 | 11/May/2032 | D/C |
| 21 | DELELIS, JOHN MARK DOMINGO | M | 23/Jan/2002 | FILIPINO | P7274860B | 26/Jul/2031 | E/C |

I certify that the above information is, to the best of my knowledge & belief, true in every particular.

Dated this__day of

Master/~~Owner/Charterer/Agent~~

*Delete whichever is inapplicable.
Note: If the spaces provided are insufficient, use an additional sheet drawn in the same format and with the "Form 22 Continued"

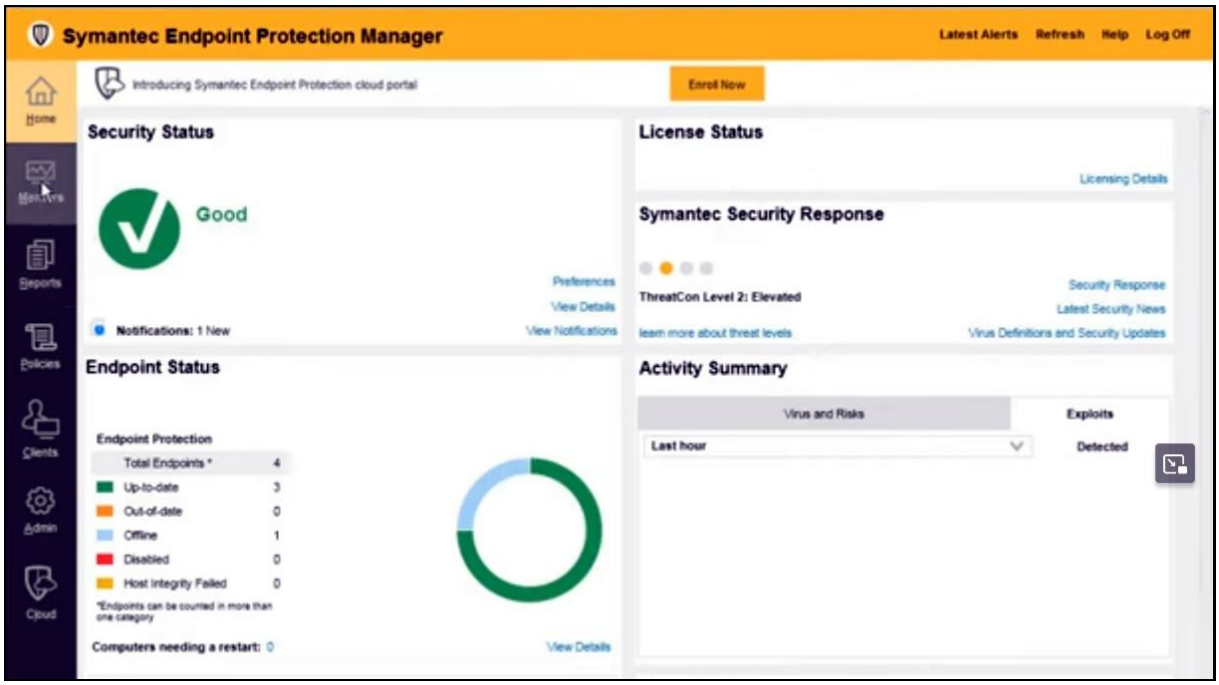
IMM 22

**LAMPIRAN 3**

MV. EVER OCEAN

# LAMPIRAN 4

*SymantecEndpoint Protection Manager*



# LAMPIRAN 5

*Reiterate Two Best Practices to Eliminate Cyber Risk of USB Devices*

EVERGREEN GROUP **MARINE CIRCULAR**



**TO:** Fleet vessels

**DATE:** Jun /09 /2023

**REF. NO.:** 2023-020

**SUBJECT:** Reiterate Two Best Practices to eliminate Cyber Risk of USB devices

MESSAGE:

Computer Viruses of USB devices are identified as one of the biggest threats of Cyber Risk Management on Evergreen fleet vessels. MAT has issued "**Two best practices to eliminate Cyber Risk of USB devices**" (see Annex-1) for crew to refer and to implement. Recently, it was found that the event of virus detection was occurred frequently since this procedure was not followed completely by some crew, which also aroused company management concern.

USB 裝置的電腦病毒為長榮船隊網絡風險管理的最大威脅，MAT 據此已發佈"**Two best practices to eliminate Cyber Risk of USB devices**"程序(參考 Annex-1)供船隊參考與實施。近期發現由於部分船員未能遵照此程序以致病毒事件頻繁發生，也同時引起公司管理階層關注。

The most serious punishment so far is **direct dismissal** for office employees who violate the company's Information Security Policy, Rules of Use Electronic Information System, or fail to comply with relevant procedures.

岸端辦公室員工違反公司資訊安全政策、電子資訊系統使用規則，或是不遵守相關程序，到目前為止最嚴重之處分是**直接予以免職**。

In order to comply with Fleet Cyber Risk Management and to reduce the cyber risk of USB devices effectively, MAT hereby reiterate that the procedure of **"Two best practices to eliminate Cyber Risk of USB devices" must be fully implemented**. If any non-compliance is found, unless there are special circumstances or any particular reasons, formal disciplinary action will be taken as a violation of the company Information Security regulations.

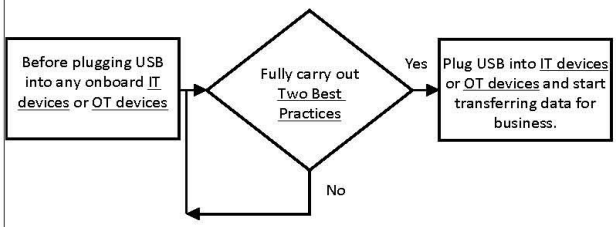
為符合船隊網絡風險管理並有效降低 USB 裝置風險，MAT 特此重申**"Two best practices to eliminate Cyber Risk of USB devices"程序必須確實落實**，如發現任何因未遵守情事，除非有特殊情況或是原因，否則將比照違反公司資訊安全規定，給予正式懲戒議處。

The following example 1 is the procedure for plugging "**a registered USB device**" into IT or OT devices. The example 2 is the procedure for transferring scrubber data from "SOX Scrubber main control panel (OT)" to "an office computer (IT)" by "a registered USB device". Both procedures are also applicable to all onboard IT or OT devices, such as updating charts on ECDIS and so on.

以下範例一為使用"已註冊 USB 裝置"接上 IT 設備或 OT 設備之程序；範例二為使用"已註冊 USB 裝置"將船端脫硫設備(OT)之數據轉存至辦公室電腦(IT)之程序。此程序一併適用其他 IT/OT 設備，例如 ECDIS 電子海圖圖資更新也一併適用。

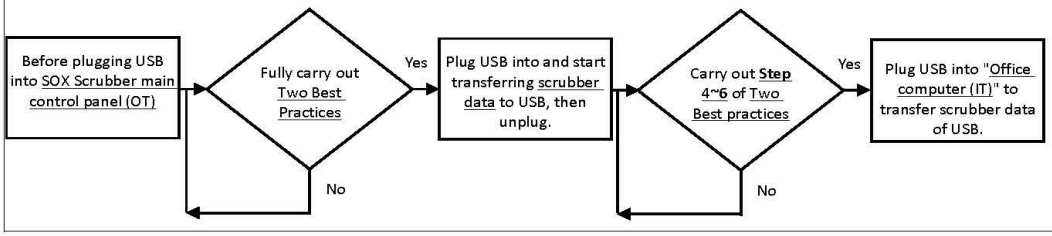
| Higher Cyber Risk | Lower Cyber Risk |
|---|---|

Example 1:




| Higher Cyber Risk | Lower Cyber Risk | Higher Cyber Risk | Lower Cyber Risk |
|---|---|---|---|

Example 2:




Your kind attention and cooperation would be highly appreciated.
感謝您的合作

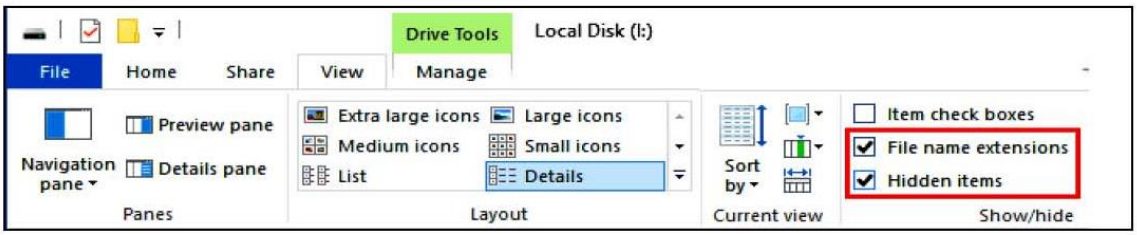
Bon Voyage.
順頌　航安！

**Annex-1 Two Best Practices to eliminate Cyber Risk of USB devices**

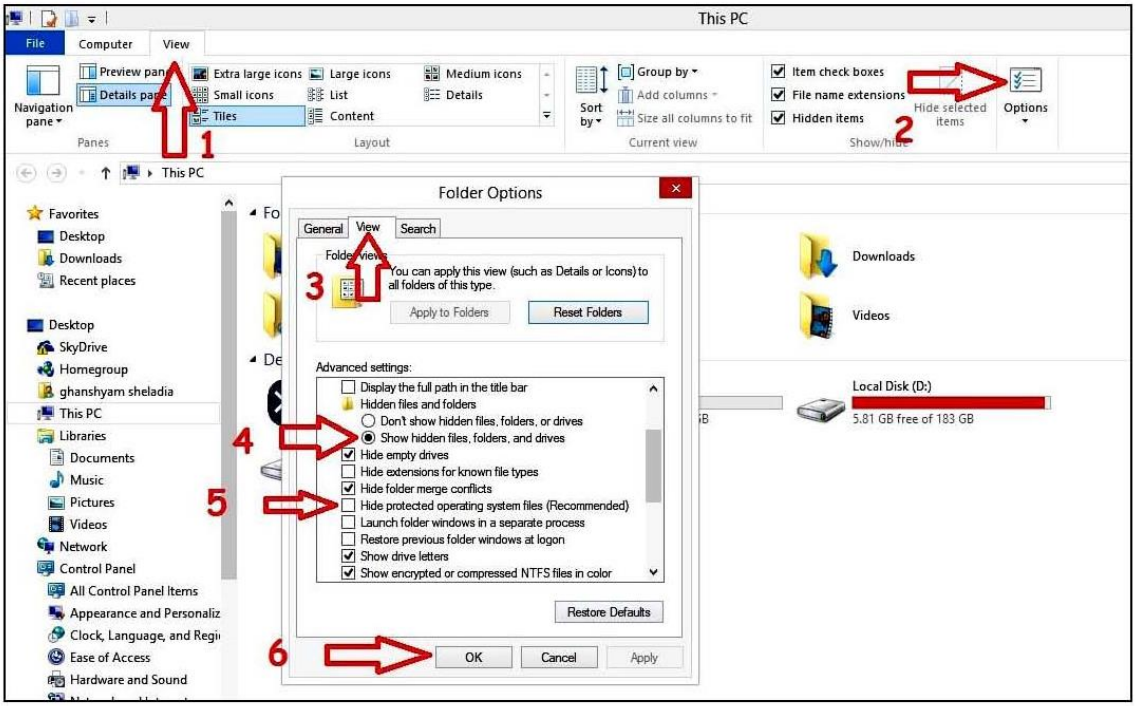
| | |
|---|---|
| ➢ **Before connect "an office camera" to "an office computer (IT)" 將"公用相機"連接"辦公用電腦(IT)"之前** | |
| Cyber Risk: | The **internal memory (built-in)** and **memory card** might contain viruses once an office camera was connected to **any non-office computers**.<br>相機之**內建記憶體**與**外接記憶卡**一旦連接過任何**非辦公用電腦**皆可能含有病毒。 |
| Best practice: | Always format both **internal memory (built-in)** and **memory card** by the office camera before taking a photo.<br>拍照前使用公用相機內建功能進行**內建記憶體**與**外接記憶卡**之格式化作業。 |
| ➢ **Before plug "a registered USB device" into "an office computer (IT)" 將"已註冊 USB 裝置"連接"辦公用電腦(IT)"之前** | |
| Cyber Risk: | **A registered USB device** might contain viruses once connected to **any non-office computers**.<br>**已註冊 USB 裝置**一旦連接過任何**非辦公用電腦**皆可能含有病毒。 |
| Best practice: | **[Format]**<br>1. Format after plugging the registered USB into **the non-office computer**.<br>將已註冊 USB 裝置插上**非辦公用電腦**後並執行格式化作業。<br>**[Virus scan]**<br>2. **Virus scan** after plugging the registered USB into **the non-office computer** (if any).<br>將已註冊 USB 裝置插上**非辦公用電腦**後並執行掃毒作業 (如有的話)。<br>**[Transfer files]**<br>3. Transfer files of business use between the registered USB and **non-office computer**.<br>於已註冊 USB 裝置與**非辦公用電腦**之間傳送公務用檔案。<br>**[Show & Delete files]**<br>4. Refer to **Steps for showing "File name extensions & "Hidden files, folders, drivers** (see Annex-2) to check if any unusual hidden files remain in the registered USB, especially file name extensions such as "***.exe***", "***.lnk***", "***.js***", "***.inf***", "***.vbs***", etc., which should not contain in this USB device.<br>參考**顯示隱藏的檔案、資料及磁碟機之步驟**(參考 Annex-2)並檢查已註冊 USB 內是否存有任何不必要的隱藏檔，特別是附檔名為"***.exe***"、"***.lnk***"、"***.js***"、"***.inf***"、"***.vbs***"等皆不應留存於 USB 裝置內。<br>5. Delete all unusual hidden files and unplug the registered USB.<br>刪除所有不必要的隱藏檔並卸除該已註冊 USB 裝置。<br>**[Check again]**<br>6. Plug the registered USB into **the non-office computer again** and check if any unusual hidden files regenerated. **If yes, do not plug into "office computers (IT)"** because of cyber risks.<br>再次將該已註冊 USB 裝置插上**非辦公用電腦**並檢查是否有不必要的隱藏檔產生。**如有的話，勿插上"辦公用電腦(IT)"**因有風險。 |

## Annex-2 Steps for showing "File name extensions" & "Hidden files, folders, drivers"

1. Enable "**File name extensions**" and "**Hidden items**".


2. Enable "**Show hidden files, folders, and drives**" and uncheck "**Hide protected operating system files (Recommended)**".



**LAMPIRAN 6**

*USB Mass Storage Device Management Onboard Fleet Vessels*

EVERGREEN GROUP **MARINE CIRCULAR**



**TO: Fleet vessels**

**DATE: JUN / 09 /2023**
**REF. NO. : 2023-010**

---

**SUBJECT: USB mass storage device management onboard fleet vessels**
**船隊 USB 存取裝置管理規則**

MESSAGE:

Using USB mass storage devices onboard ship may seem innocuous due to the convenience of Plug-and-Play, but it has the potential to cause many problems and will increase cyber risks for all computer system onboard ship. Many studies have reported that there are a large number of malwares spread today through USB devices.
由於存取方便，看似無害的USB存取設備，往往讓人們忽略了其背後的潛在危害，以及對船上電腦系統可能造成的資安風險，許多研究都表明，USB裝置是惡意軟體的主要傳播途徑。

After reviewing recent records of cyber incident in our fleet, we found that the major cause of these incidents is **improper use of USB mass storage devices**. MAT hereby establishes the Regulations of USB mass storage device management onboard for company's fleet to obey.
經檢視近期船隊資安事件後，我們發現「**不當使用USB裝置**」是船隊資安的主要威脅，海技部特此制定船隊USB存取裝置管理規則，屬輪應落實遵守本規則之各項規定。

The "Regulations of USB mass storage device management onboard fleet vessel" shall **become effective from Apr. 6, 2020**, and it shall be printed out for future reference. Meanwhile, it shall be included in the agenda of Shipboard Monthly Meeting next monthly.
**本管理規則自2020年4月6日起生效實施**。規則本文請列印後備查，並於下次月會中進行討論。

You have been warned!! The violators in breaching the requirements of USB mass storage device management onboard fleet vessels **who will be subjected to disciplinary measures up to and including dismissal**, and will also look into the **Master's administrative responsibility** thereof.
請注意!!如有船員違反船隊USB裝置管理規定，除**嚴懲相關失職人員**外，將**追究該輪船長之行政管理責任**。

Bon Voyage.
順頌 航安！

# Regulations of USB mass storage device management onboard fleet vessels
# 船隊USB存取裝置管理規則

1. The provisions in this regulation provide, if necessary, to the crew members uses USB mass storage device for comply with the requirements of Company and to avoid unauthorized use and misuse.
為使船隊USB存取裝置之使用符合公司規範，並避免未經授權的使用與濫用，特制定本規則。

2. The definition of the terms referred to in this regulation are as follows:
本規則用詞，定義如下：

   a. **Official business** means business pertaining to or required by the duties;
   **公務**是指與職責所需或相關的業務。

   b. **USB mass storage device** (hereinafter called USB device) means all devices connected to computers via USB MSC standard, include：
   USB存取裝置（後稱USB裝置）指所有利用USB MSC標準埠與電腦連接之下列裝置：
   - External hard drives, including Solid-state drives　外接式硬碟（含固態硬碟）；
   - External optical drives, including CD and DVD reader/writer drives　外接式光碟機；
   - Portable flash memory devices　隨身碟；
   - Digital cameras　數位相機；
   - Digital audio and portable media players　可攜式媒體播放器；
   - Card readers　讀卡機；
   - PDAs　個人數位助理；
   - Smartphones　智慧型手機；and
   - Wireless network interface controller　無線網卡。

   c. **Operational technology (hereinafter called OT)**
   OT is used to manage physical processes and actuation through the direct sensing, monitoring and or control of physical devices, for example, motors, valves, pumps, etc. In a vessel computers may include, but is not limited to：ICMS, computers using for monitoring of running of main/auxiliary engines in engine room, reefer container monitoring system, ballast water management system, navigational equipment in bridge etc.
   操作型技術系統（後稱OT電腦）是指用以直接感測、監視與控制物理設備（如馬達、閥門、泵等）來管理並作動該設備的電腦系統，船上OT電腦包含但不限於：ICMS、機艙之主／輔機監控電腦系統、冷凍櫃監控系統、壓艙水管理系統、駕駛台航儀設備等。

   d. **Information Technology (hereinafter called IT)**
   IT is the use of computers to store, retrieve, transmit, and manipulate data or information. In a vessel these computers may include, but is not limited to：Master's communication computers, Cargo computer, public computers in deck office/engine control room and official computers in key members cabin etc.

資訊技術系統（後稱IT電腦）是指用於儲存、檢索、傳輸與處理資料和信息的電腦系統，船上IT電腦包含但不限於下列：船長通信電腦、算貨電腦、辦公室公務用電腦與主管房間裡的公務電腦等。

3. The IT computers onboard are required to keep the definition of anti-virus software updated and conduct a fully scan regularly. The status of Symantec Endpoint protection for all IT computers onboard shall be reported to MAT by the end of each month.
船上IT電腦應及時更新防病毒軟件定義檔，並定期執行完整掃毒功能，屬輪應於每月底前回報船上所有IT電腦的防毒軟體狀態給海技部。

4. The Second Officer, under Master's supervision is responsible for maintaining a log, which is maintained to register all **USB devices that is using for official business onboard** (Attachment 1). This log shall be updated subject to change of listed information and then submitted to MAT for filing.
二副應在船長監督下列表管理**船上公務用USB裝置**（附件一），表單資訊如有變動應隨時更新並回報海技部備查。

5. The USB device which intended for use in official business onboard is required to register in the log aforesaid and then it is allowed to use. The holder shall **format** the USB device on a computer which installed with updated Anti-Virus software, and **follow by a Scan for Viruses**. After confirming that the USB device is free from viruses, the holders shall provide required information to Second Officer for registry. The registered USB device shall be labeled by its number as identification.
USB裝置須經登錄在冊，方得在船上為公務使用。持有人應先在有及時更新防毒定義檔的電腦上**格式化該USB裝置**，並**執行掃毒**，確認該裝置無電腦病毒後，提報相關資訊給二副登錄於登記表內，並標示其編號以為識別。

6. **Any unregistered USB device connects to shipboard computers is strictly prohibited,** except as otherwise specifically provided herein.
除本規則另有規定外，**未登錄於表內的USB裝置禁止使用。**

7. Requirements for using USB device onboard
船上USB裝置使用規定

   a. The OT computers are not allowed to use USB device except an authorization from ship's Master have been obtained.
   除經船長授權外，船上 OT 電腦禁止使用 USB 裝置；

   b. USB devices can only be used on the **dedicated IT computer** after accessing the Electronic Information System (EIS) by **logging in an authorized EIS account**.
   只允許在**專用的 IT 電腦上登錄公司授權的 EIS 帳號後**，方得使用 USB 裝置；

   c. The user is required to **manually conduct a Scan for Viruses immediately** after connecting the USB

device with IT computer **every single time**. (With the USB drive plugged in, open My Computer. Right-click on the USB icon, then left-click Scan for viruses from the drop-down menu.)
**每次**將USB裝置插入IT電腦時，應立即執行**手動掃毒**（插入USB→從檔案管理員找到該USB裝置→滑鼠移至該裝置後按右鍵→點選Scan for Viruses）；

d. You are forbidden from executing, copying, installing and downloading unauthorized software and files by using USB devices.
禁止使用USB裝置執行、複製、安裝和傳輸未經授權的軟體與檔案；

e. The data and files kept in the registered USB device shall be limited to official business only, which are prohibited to mix with unofficial files, illegal software, e-books, computer games and audio-visual files etc.
公務用USB裝置應僅用於存取公務檔案，避免混雜非公務檔案、非法軟件、電子書、遊戲與影音檔案等；

f. Crew members shall immediately log out the EIS account after completing the use of USB device. You are forbidden from "providing your password to any other person unauthorized".
USB裝置使用完畢後，應立即登出EIS授權帳號，禁止將系統帳密提供他人使用。

8. If there is a printing or file transferring request from external parties, the files should be sent to the Master's official e-mail address for the said purposes, using USB device is prohibited, **except the request from cargo planner or official authorities**.
**除Cargo Planner、官方與主管單位**外，如外部單位有列印或檔案傳輸的需求，應將檔案以電郵發送到船上公務信箱後再行處理，禁止使用USB裝置傳輸檔案。

9. In case of an emergency or under other special circumstances, the use of USB device is allowed in accordance with the rule 7 of this regulation after obtaining authorization from ship's Master. This operation shall be reported to MAT without delay.
緊急或特殊狀況下，經取得船長同意，得依本規則第7條之規定使用USB裝置。船長應盡速以書面報告向海技部回報前述操作的相關說明。

10. You are required to immediately implement below procedures once there are viruses or suspect files detected on the USB device in using.
一旦USB裝置遭偵測到含有電腦病毒或可疑檔案時，應立即採取下列程序：

a. Remove the USB device from computer.
立即移除該USB裝置；

b. Manually conduct a Run Full Scan by Symantec Endpoint protection.
立即手動執行防毒軟體的Run Full Scan掃毒程序；

c. Report required information to MAT as follows, after the Run Full Scan completed.
Run Full Scan掃毒程序完成後，回報下列資訊給海技部；

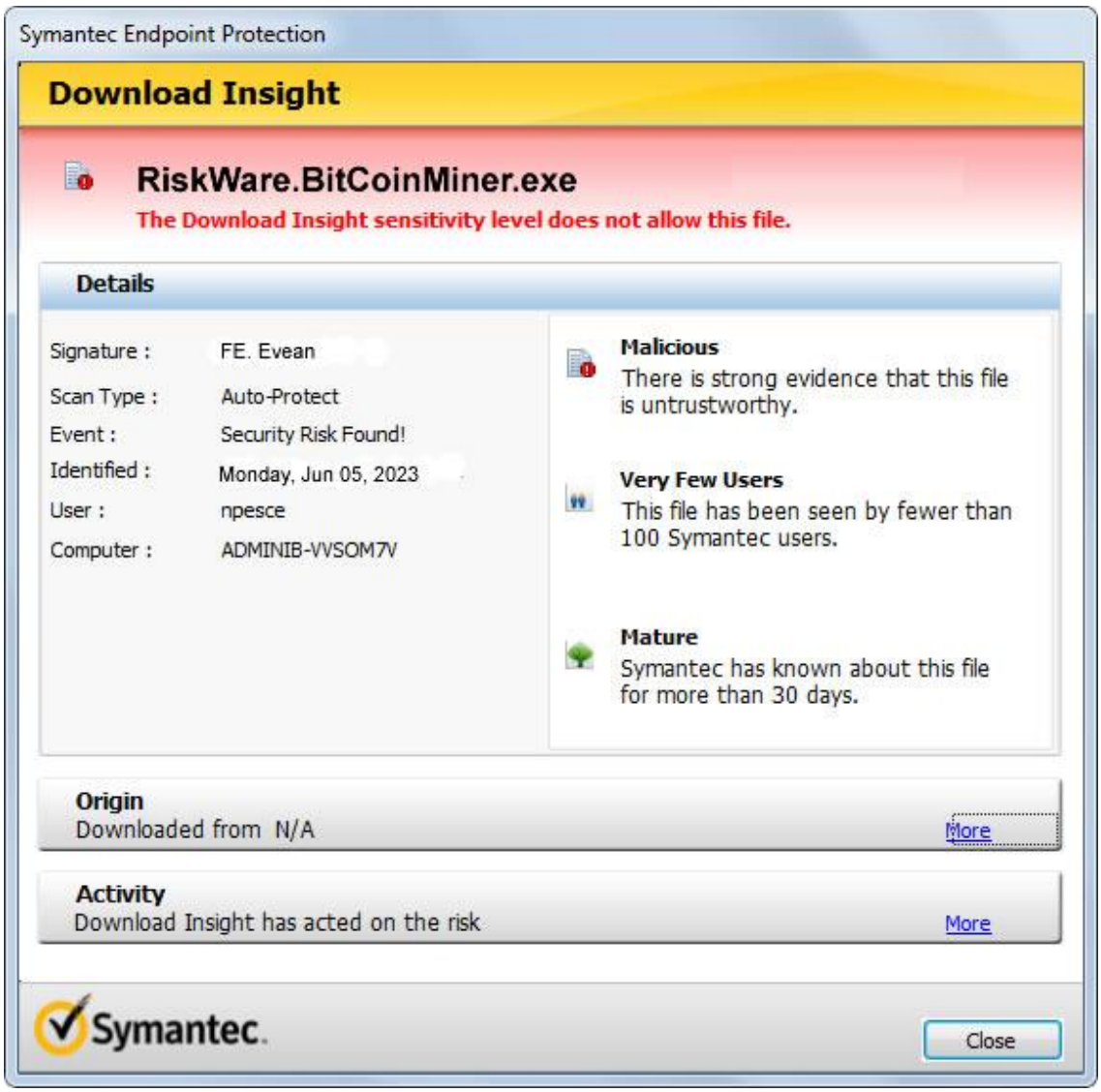
- Master shall investigate the incident and a short statement is required that should include how and when the incident was initially detected, who experienced the incident and his purpose, details of device, the suspected source of viruses and a screen shot of the Status of Symantec Endpoint protection etc.
船長應立即著手調查事件始末，簡要說明事發時間、人員、目的、裝置明細與可能感染源等，並附上電腦防毒軟體狀態截圖；
- Export the CSV file of Risk Log of Symantec Endpoint protection,
匯出電腦防毒軟體的Risk Log（CSV檔）；
- Export the CSV file of Scan Log of Symantec Endpoint protection.
匯出電腦防毒軟體的Scan Log（CSV檔）；

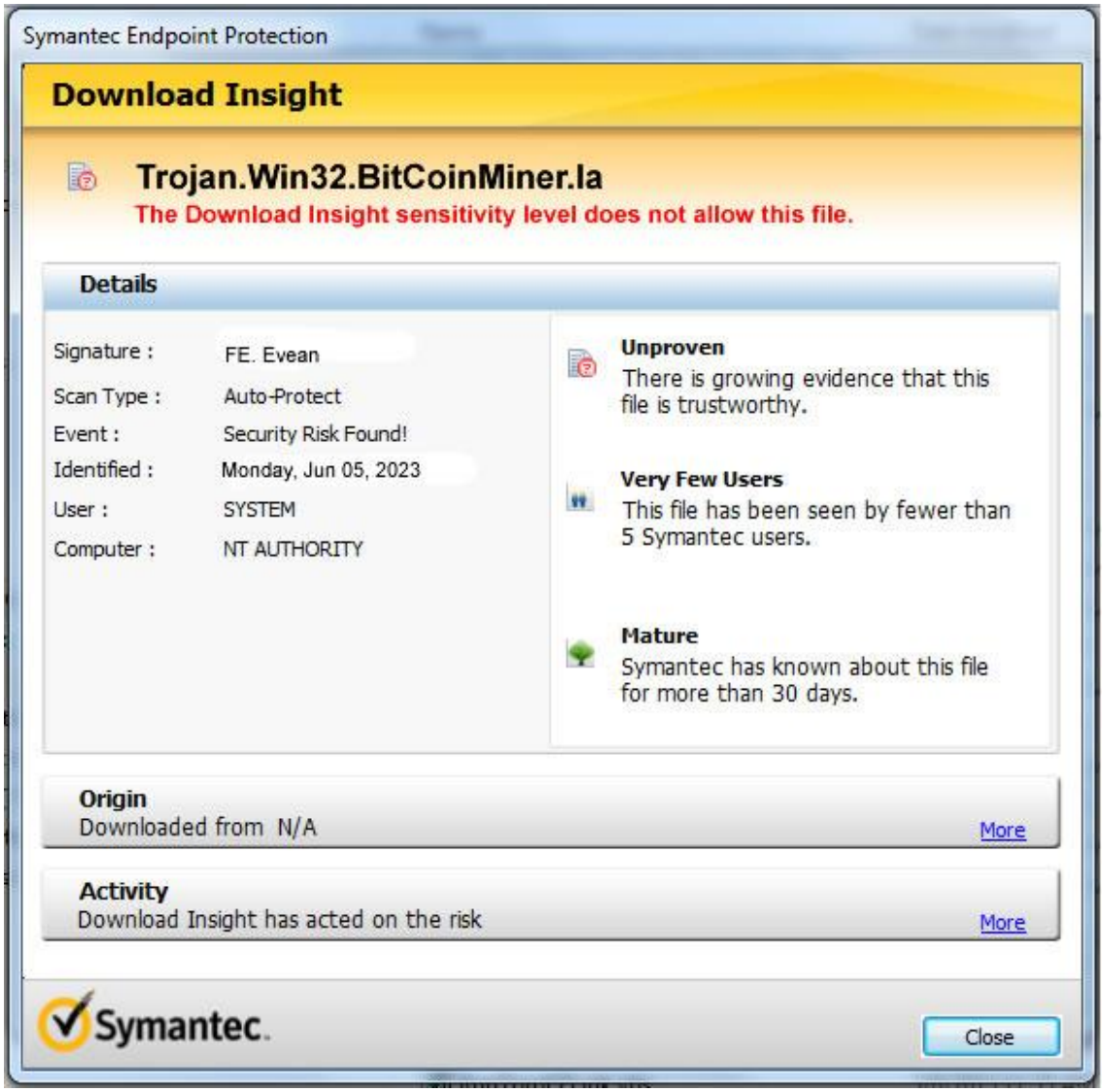
d. Use the virus infected USB device on any shipboard computer is prohibited without further instruction from company.
在獲得公司進一步指示前，禁止於任何電腦（含OT與IT）上使用該USB裝置。

**LAMPIRAN 7**



Jenis Virus *Cryptocurrency Miner*




Symantec Endpoint Protection
Download Insight
Trojan.Win32.BitCoinMiner.la
The Download Insight sensitivity level does not allow this file.
Details
Signature : FE. Evean
Scan Type : Auto-Protect
Event : Security Risk Found!
Identified : Monday, Jun 05, 2023
User : SYSTEM
Computer : NT AUTHORITY
Unproven
There is growing evidence that this file is trustworthy.
Very Few Users
This file has been seen by fewer than 5 Symantec users.
Mature
Symantec has known about this file for more than 30 days.
Origin
Downloaded from N/A
More
Activity
Download Insight has acted on the risk
More
Symantec.
Close

# DAFTAR ISTILAH

| | | |
|---|---|---|
| *Advanced Persistent Threat* (APT) | : | serangan yang dilakukan oleh penyerang yang terorganisir dan sangat terlatih dengan tujuan mencuri informasi berharga atau mengganggu operasi organisasi. APT seringkali berlangsung dalam jangka waktu yang lama dan sulit dideteksi. |
| *Business Continuity Planning* (BCP) | : | proses perencanaan dan persiapan untuk menjaga kelangsungan operasional organisasi dalam menghadapi insiden keamanan atau bencana. |
| *Compliance* | : | kepatuhan terhadap peraturan, standar, dan peraturan yang berkaitan dengan keamanan cyber, seperti GDPR (General Data Protection Regulation) di Uni Eropa atau HIPAA (Health Insurance Portability and Accountability Act) di Amerika Serikat. |
| *Cyber Risk* | : | risiko yang timbul dari serangan atau ancaman terhadap sistem komputer, jaringan, atau data yang dapat menyebabkan kerugian finansial, reputasi, atau operasional. |
| *Encryption* | : | proses mengubah data menjadi format yang tidak dapat dibaca atau dimengerti oleh pihak yang tidak berwenang, menggunakan algoritma enkripsi dan kunci untuk melindungi kerahasiaan data. |

*Firewall* : sistem keamanan yang digunakan untuk memonitor dan mengontrol lalu lintas jaringan, membatasi akses yang tidak sah atau berbahaya antara jaringan internal dan eksternal.

*Incident Response* : proses yang melibatkan identifikasi, respons, dan pemulihan setelah terjadi insiden keamanan, seperti serangan malware atau pelanggaran data.

*Insider Threat* : ancaman yang berasal dari dalam organisasi, yaitu individu yang memiliki akses terotorisasi ke sistem dan memanfaatkannya dengan tujuan merusak, mencuri data, atau memberikan informasi rahasia kepada pihak ketiga.

*Intrusion Detection System* (IDS) : sistem yang dirancang untuk mendeteksi dan merespons serangan atau aktivitas mencurigakan dalam jaringan atau sistem komputer.

*Malware* : singkatan dari "malicious software" atau perangkat lunak berbahaya yang dirancang untuk merusak, mencuri informasi, atau mengganggu sistem komputer. Contoh malware termasuk virus, worm, Trojan, ransomware, dan spyware.

*Man-in-the-Middle* (MitM) *Attack* : serangan di mana penyerang memposisikan dirinya di tengah komunikasi antara dua pihak yang sah, dengan tujuan memantau, memodifikasi, atau mencuri data yang sedang

dipertukarkan.

*Penetration Testing* : proses di mana seorang profesional keamanan mencoba untuk mengevaluasi kelemahan dalam sistem atau jaringan dengan menguji serangan seperti serangan DDoS, eksploitasi kelemahan, atau upaya phishing.

*Phishing* : teknik penipuan di mana penyerang mencoba untuk memperoleh informasi sensitif seperti kata sandi, nomor kartu kredit, atau informasi pribadi dengan menyamar sebagai entitas tepercaya melalui email, pesan teks, atau situs web palsu.

*Ransomware* : jenis malware yang mengenkripsi data pada sistem korban dan menuntut pembayaran tebusan agar data dapat di-dekripsi dan diakses kembali. Pembayaran biasanya diminta dalam bentuk cryptocurrency.

*Risk Appetite* : tingkat risiko yang dapat diterima oleh organisasi dalam hal keamanan cyber, berdasarkan pada tujuan bisnis, sumber daya, dan toleransi terhadap kerugian potensial.

*Risk Assessment* : proses identifikasi, evaluasi, dan analisis risiko cyber untuk menentukan tingkat kerentanan dan dampak potensial terhadap organisasi.

*Risk Mitigation* : tindakan atau strategi untuk mengurangi

atau meminimalkan risiko cyber, termasuk penerapan kontrol keamanan, kebijakan, dan tindakan perlindungan.

*Risk Monitoring* : pemantauan terus-menerus terhadap risiko cyber untuk mengidentifikasi perubahan atau ancaman baru yang mungkin muncul, dan mengambil tindakan yang sesuai.

*Security Governance* : kerangka kerja dan proses yang mengatur pengelolaan keamanan cyber di seluruh organisasi, termasuk kebijakan, prosedur, dan tanggung jawab yang terkait.

*Social Engineering* : pendekatan psikologis yang digunakan oleh penyerang untuk memanipulasi orang agar mengungkapkan informasi rahasia atau memberikan akses tidak sah ke sistem. Contoh teknik social engineering termasuk pretexting, phishing, atau insinuasi.

*Threat* : potensi ancaman yang dapat menyebabkan kerugian atau kerentanan dalam sistem atau jaringan, seperti serangan malware, serangan DDoS, atau serangan phishing.

*Vulnerability* : kelemahan atau celah dalam sistem komputer atau jaringan yang dapat dieksploitasi oleh penyerang untuk merusak atau mengakses data secara tidak

KEMENTERIAN PERHUBUNGAN
BADAN PENGEMBANGAN SUMBER DAYA MANUSIA PERHUBUNGAN
SEKOLAH TINGGI ILMU PELAYARAN
PROGRAM DIKLAT PELAUT
JAKARTA

# PENGAJUAN SINOPSIS MAKALAH

NAMA : Over Grand Hutauruk
NIS : 02876 / N-I
Bidang Keahlian : NAUTIKA
Program Diklat : DIKLAT PELAUT - I

**Mengajukan Sinopsis Makalah Sebagai Berikut**

A. Judul : PENERAPAN MANAJEMEN RISIKO CYBER SECURITY DIATAS MV. EVER OCEAN UNTUK MEWUJUDKAN KEAMANAN TEKNOLOGI INFORMASI DIERA SOCIETY 5.0

B. Masalah Pokok :

1. Faktor yang mengakibatkan kurangnya pemahaman Crew terhadap *Cyber Security* diatas kapal khususnya *Fleet Evergreen* Sehingga berdampak pada bocornya data data perusahaan.
2. Dampak yang terjadi pada saat terdeteksi Virus tertentu sehingga menyebabkan turunnya kinerja komputerisasi yang ada diatas kapal Evergreen seperti akses komunikasi antara kapal dengan perusahaan maupun pihak yang terkait dengan operational kapal dipelabuhan maupun otoritas.

C. Pendekatan Pemecahan Masalah

1. Melakukan edukasi / training untuk Crew Kapal Evergreen mengenai " Prosedur penerapan *Cyber Security training* "
2. Melakukan Download & Update Virus untuk semua komputer diatas kapal seperti Symantec dengan rutin guna menghambat adanya serangan virus dari *hard drive* atau USB untuk optimalisasi kinerja komputer kapal yang lebih baik.
3. Adanya registrasi USB / Hard drive dari setiap Crew Evergreen Fleet untuk menghindari adanya *illegal login* masuk kesistem komputer kapal sehingga menjaga *Cyber security* kapal aman dan mudah untuk dideteksi oleh *Ship Cyber Security Officer* ( SCSO ) .
4. Memberikan laporan ke *Ship Cyber Security Officer* ( SCSO) secara berskala mengenai " *Risk Assessment for Cyber Security*" setiap adanya pergantian crew diatas kapal.

Jakarta, 29 Agustus 2023

Menyetujui :

| Pembimbing I | Pembimbing II | Peserta Diklat Pelaut ( DP-I ) |
|---|---|---|
| **Bhima Siswo Putro, S.SIT.,MM** | **Ronald Simanjuntak, M.T.** | **Over Grand Hutauruk** |
| Penata TK.1 ( III/c ) | Pembina ( IV/A ) | NIS. 02876 / N-I |
| NIP.19730526 200812 1 001 P206922 | NIP.19750616 200604 1 001 | |

Kepala Divisi Pengembangan Usaha

**Capt. SUHARTINI, MM, MMTr**
Penata Tk.I (III/D)
NIP. 19800307 200502 2 002

SEKOLAH TINGGI ILMU PELAYARAN

DIVISI PENGEMBANGAN USAHA

PROGRAM DIKLAT PELAUT - I

JUDUL MAKALAH :

PENERAPAN MANAJEMEN RESIKO *CYBER SECURITY* DI ATAS KAPAL KHUSUSNYA *FLEET* EVERGREEN UNTUK MEWUJUDKAN KEAMANAN TEKNOLOGI INFORMASI DIERA *SOCIETY 5.0*

DOSEN PEMBIMBING MATERI : Bhima Siswo Putro, S.SIT.,MM

MATERI BIMBINGAN :

| NO | TANGGAL | URAIAN MATERI | TANDA TANGAN PEMBIMBING |
|---|---|---|---|
| | 16/08 2023 | Pengajuan judul | |
| | 24/8 '23 | Bab I. Revisi. | |
| | 25/08/23 | Bab II Revisi | |
| | 04/09 23 | Bab III Ok, Bab I Ok, Bab II Ok | |
| | | Bab IV Revisi. + Data Pelengkap. | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Catatan :

.....

.....

.....

SEKOLAH TINGGI ILMU PELAYARAN

DIVISI PENGEMBANGAN USAHA

PROGRAM DIKLAT PELAUT - I

JUDUL MAKALAH :

PENERAPAN MANAJEMEN RESIKO *CYBER SECURITY* DI ATAS KAPAL KHUSUSNYA *FLEET* EVERGREEN UNTUK MEWUJUDKAN KEAMANAN TEKNOLOGI INFORMASI DIERA *SOCIETY 5.0*

DOSEN PEMBIMBING PENULISAN : Ronald Simanjuntak, M.T.

MATERI BIMBINGAN :

| NO | TANGGAL | URAIAN MATERI | TANDA TANGAN PEMBIMBING |
|---|---|---|---|
| 1 | 16/8/23 | Sinopsis Judul | |
| 2 | 21/8/23 | Revisi untuk BAB I | |
| 3 | 25/8/23 | Perbaiki Untuk Bab II | |
| 4 | 04/9/23 | Perbaiki Resiko menjadi Risiko | |
| | | Bab III & IV perbaiki | |
| 5 | 05/9/23 | Ok untuk Bab IV | |
| | | | |
| | | | |
| | | | |
| | | | |

Catatan :

.....

.....

.....