UNIVERSITAS PERTAHANAN

IMPLEMENTASI SISTEM PENGAMANAN INFORMASI DALAM APLIKASI *INAPORTNET* UNTUK *MARITIME CYBER SECURITY*

JURNAL ILMIAH

ASMAUL MUFIDASARI
NIM: 120170302004

FAKULTAS KEAMANAN NASIONAL
PROGRAM STUDI KEAMANAN MARITIM

BOGOR

Januari 2019

IMPLEMENTASI SISTEM PENGAMANAN INFORMASI DALAM APLIKASI INAPORTNET UNTUK *MARITIME CYBER SECURITY*

INFORMATION SECURITY SYSTEM IMPLEMENTATION IN INAPORTNET FOR MARITIME CYBER SECURITY

Asmaul Mufidasari[1], Amarulla Octavian[2], Herlina Juni Saragih[3]

Universitas Pertahanan

(asmaul.mufidasari@gmail.com)

Abstrak- Perkembangan teknologi informasi dan komunikasi telah mempengaruhi domain maritim. Perkembangan ini telah membawa ancaman baru dalam domain maritim yaitu ancaman *cyber*. Inaportnet merupakan salah satu pemanfaatan teknologi informasi dan komunikasi dalam domain maritim yang dilakukan oleh Kementerian Perhubungan. Inaportnet merupakan portal elektronik berbasis internet yang mampu mengintegrasikan seluruh sistem informasi pemangku kepentingan yang ada di pelabuhan. Ancaman *cyber* dalam aplikasi Inaportnet dapat dicegah apabila mempunyai sistem pengamanan informasi yang kuat. Tujuan dari penelitian ini yaitu menjelaskan mekanisme sistem pengamanan informasi dalam aplikasi Inaportnet dan memahami aspek pendukung dan penghambat dalam sistem pengamanan informasi di aplikasi Inapornet untuk melindungi informasi dari ancaman *cyber*. Metode penelitian yang digunakan adalah kualitatif eksploratif yaitu untuk mengungkapkan alasan tertentu mengapa informasi tersebut terjadi. Sedangkan pengolahan data untuk memeriksa keabsahan data menggunakan *software* NVivo, serta analisa data menggunakan teknik *Soft System Methodology* (SSM) untuk menghasilkan hasil analisa yang lebih mendalam, serta hasil pemikiran dan analisa yang lebih terstruktur. Hasil yang didapat adalah implementasi keamanan informasi dalam aplikasi Inaportnet belum berjalan dengan baik. Walaupun secara sistem teknologi sudah memenuhi namun aspek lain yaitu kesadaran untuk keamanan informasi masih kurang, hal ini berdasarkan temuan di lapangan. Inaportnet masih belum mempunyai *Information Security Handbook*, padahal buku ini diperlukan untuk banyak hal yang mendukung sistem keamanan informasi Inaportnet. Inaportnet juga belum mempunyai jadwal rutin untuk melakukan penetration test dan patch. Oleh karena itu, sebagai pemegang kebijakan aplikasi Inaportnet Direktorat Jenderal Perhubungan Laut perlu untuk membuat Inaportnet *information security handbook* agar sistem keamanan informasinya tidak hanya baik di teknologinya saja, namun juga baik secara manajemen antar *stakeholder* dan *cyber security awareness* di tingkat individunya.

Kata Kunci: Inaportnet, Keamanan Informasi, *Maritime Cyber security*.

---

[1] Mahasiswa Program Studi Keamanan Maritim, Fakultas Keamanan Nasional, Universitas Pertahanan.

[2] Dosen Tetap Universitas Pertahanan dan Komandan Sesko TNI AL.

[3] Dosen Tetap Universitas Pertahanan dan Sesprodi Program Doktoral Manajemen Pertahanan.

Abstract- *The development of information and communication technology has influenced the maritime domain. This development has brought cyber threats in the maritime domain. Inaportnet is one of the uses of information and communication technology in the maritime domain carried out by the Ministry of Transportation. Inaportnet is an internet-based electronic portal that is able to integrate all stakeholder information systems in the port. Cyber threats in Inaportnet applications can be prevented if they have a strong information security system. The purpose of this study is to explain the mechanism of information security systems in the Inaportnet application and understand the supporting and inhibiting aspects of the information security system in the Inapornet application to protect information from cyber threats. The research method used is qualitative explorative which is to reveal certain reasons why the information occurred. While processing data to check the validity of data using NVivo software, and data analysis using Soft System Methodology (SSM) techniques to produce more in-depth analysis results, as well as more structured results of thought and analysis. The results obtained are that the implementation of information security in the Inaportnet application is not running well. Although the technology system has fulfilled but other aspects, namely awareness for information security is still lacking, this is based on findings in the field. Inaportnet still does not have the Information Security Handbook, even though this book is needed for many things that support the Inaportnet information security system. Inaportnet also does not have a routine schedule for doing penetration tests and patches. Therefore, as the holder of the Inaportnet, Directorate General of Sea Transportation application policy, it is necessary to make Inaportnet information security handbook so that the information security system is not only good in the technology, but also in management between stakeholders and cyber security awareness at the individual level.*

Keywords*: Inaportnet, Information Security, Maritime Cyber security.*

PENDAHULUAN

Pada era modern saat ini keamanan nasional tidak hanya tertuju pada segi militer saja, keamanan nasional pada era modern saat ini memiliki bentuk yang lebih global. Banyak negara yang menerapkan sistem keamanan nasional sesuai dengan perkembangan lingkungan strategis dan perkembangan ancaman yang terjadi di negaranya. Keamanan nasional dapat meliputi keselamatan dan keamanan suatu negara, melalui berbagai aspek seperti aspek militer, ekonomi, diplomasi, keamanan energi, lingkungan dan lain sebagainya. Begitupun dengan ancaman keamanan yang semula berorientasi pada ancaman tradisional, saat ini telah beralih menjadi ancaman yang lebih multidimensi.[4] Gagasan tentang keamanan nasional termasuk salah satu gagasan baru. Keamanan Nasional sering mengacu pada negara merdeka yang berusaha melindungi integritas dan wilayah teritorialnya.

[4] Bambang Darmono, "Konsep dan Sistem Keamanan Nasional Indonesia", *Jurnal Ketahanan Nasional*, Volume 15 (1), 2010, hlm. 1.

Definisi keamanan nasional dapat seringkali dikaitkan dengan kemampuan suatu negara dalam melindungi negaranya dari ancaman yang datang dari luar. Keamanan nasional sendiri merupakan keamanan suatu negara, keamanan nasional dan integritas keamanannya serta kedaulatannya.[5]

Keamanan nasional dipengaruhi oleh dinamika perubahan dalam lingkungan strategi atau faktor-faktor dari dalam negeri yaitu ideologi, politik, ekonomi, sosial, budaya, pertahanan dan keamanan.[6] Seiring dengan perkembangan teknologi informasi dan komunikasi yang saat ini telah dimanfaatkan dalam berbagai sektor lingkungan strategis menyebabkan perkembangan baru dalam dinamika lingkungan strategis tersebut. Akibat pengaruh dari teknologi informasi dan komunikasi seluruh dimensi lingkungan strategis telah terkonversi kedalam dunia *cyber space*. Keberadaan *cyber space* yang lebih mudah dijangkau dan diakses harus diimbangi dengan kemampuan negara dalam menguasai, mengawasi, dan mengendalikan pergerakannya dalam dunia *cyber*. Perkembangan teknologi informasi dan komunikasi dapat menjadi sarana baru untuk melakukan berbagai penetrasi, pengaruh dan infiltrasi ke berbagai lingkungan strategis yang ada di Indonesia. Dengan wilayah Indonesia yang didominasi oleh laut, maka pengaruh dari lingkungan strategis juga dipengaruhi oleh kondisi Indonesia yang didominasi oleh wilayah laut.

Wilayah laut yang luas dan berbentuk pulau-pulau membuat Indonesia sangat rentan terhadap ancaman, baik ancaman militer maupun non-militer. Oleh karena itu, perkembangan Keamanan Nasional Indonesia juga dipengaruhi oleh posisi Indonesia sebagai negara kepulauan dan mempunyai wilayah laut yang luas. Oleh sebab itu, pembahasan tentang isu-isu dalam keamanan maritim sedang menjadi perhatian internasional. Menurut Bueger (2015) perbincangan tentang keamanan maritim sering merujuk pada 'ancaman' yang berlaku di domain maritim. Persoalan dalam keamanan maritim menyangkut banyak aspek seperti lingkungan laut, pengembangan ekonomi, keamanan nasional, dan *human security*. Keamanan maritim merupakan

[5] Natasha Grozdanoska, "National Defence and Security", *European Scientific Journal*, Volume.1, 2014, ISSN-1857-7431

[6] Kementerian Pertahanan Indonesia, "Buku Putih Pertahanan Indonesia", 2015, hlm 1.

sebuah kata kunci, oleh karena itu tidak ada definisi yang pasti mengenai keamanan maritim itu sendiri.[7] Keamanan maritim modern telah dipengaruhi oleh arus globalisasi dan perkembangan teknologi. Globalisasi membawa dunia modern pada perkembangan era informasi dan komunikasi yang menciptakan era serba digital (*digital world*).

Beralihnya sistem administrasi di pelabuhan dari sistem administrasi konvensional menuju digital telah menyebabkan resiko baru, berupa kerentanan pencurian data melalui jaringan *cyber*. Walaupun ranah *maritime cyber* masih terbilang baru, namun dampak yang dihasilkan apabila terjadi kejahatan *cyber* dalam domain maritim bisa sangat besar. Disinilah peran dari penguatan *Maritime Cyber security* untuk pengamanan arus informasi digital yang berkaitan dengan domain maritim. Komputerisasi di pelabuhan ini dilakukan agar pelabuhan di Indonesia dapat berjalan cepat, efektif, efisien serta berdaya saing. Teknologi informasi dan komukasi yang dilakukan berupa penerapan portal elektronik berbasis internet yang mampu mengintegrasikan seluruh sistem informasi pemaku kepentingan yang ada di pelabuhan. Sistem ini diberi nama aplikasi Inaportnet. Inaportnet merupakan sebuah program dari Kementerian Perhubungan yang dalam implementasinya perlu dukungan bersama dari para *stakeholder* di pelabuhan serta penyelenggaraannya dilakukan oleh Direktorat Jenderal Perhubungan Laut.

Inaportnet merupakan sebuah sistem informasi layanan tunggal elektronik berbasis internet untuk mengintegrasikan sistem informasi kepelabuhanan yang standar dalam melayani kapal dan barang dari seluruh instansi terkait di pelabuhan.[8] Sesuai dengan Peraturan Menteri Perhubungan Nomor PM 157 Tahun 2015 tentang Penerapan Inaportnet untuk Pelayanan Kapal dan Barang di Pelabuhan, pada pasal 2 ayat (3) yang menyatakan penerapan Inaportnet pelayanan kapal dan barang dipelabuhan dilakukan sesuai tugas, fungsi, kewenangan, dan tanggung jawab dari setiap instansi

[7] Christian Bueger, "What is *Maritime* Security?", *Marine Policy*,Vol.53, 2014, hlm. 159.

[8] Peraturan Menteri Perhubungan RI Nomor PM 157 Tahun 2015 tentang Penerapan Inaportnet untuk Pelayanan Kapal dan Barang di Pelabuhan.

Pemerintah dan pemangku kepentingan terkait di pelabuhan berdasarkan ketentuan peraturan perundang-undangan.

Tujuan dari penelitian ini adalah untuk mengetahui implementasi sistem pengamanan informasi dalam aplikasi Inaportnet untuk *Maritime Cyber security*. Secara khusus tujuan penelitian ini ialah menganalisis mekanisme sistem pengamanan informasi dalam aplikasi Inaportnet untuk *Maritime Cyber security* dan mengalisis apa saja aspek pendukung dan penghambat dalam sistem pengamanan informasi untuk melindungi informasi dari ancaman *cyber* dalam aplikasi Inaportnet.

METODOLOGI PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan *explanatory*, yaitu penelitian dilakukan untuk mengetahui mengapa dan bagaimana fenomena-fenomena sosial terjadi diantara variabel-variabel penelitian serta menjelaskan dan/atau mengidentifikasi pola, tema yang berhubungan dengan fenomena/masalah penelitian.[9]

Pengumpulan data dilaksanakan melalui wawancara dengan beberapa informan diantaranya seperti Direktorat Jenderal Perhubungan Laut pada bagian Direktorat Lalu Lintas dan Angkutan Laut, Sekretariat Perhubungan pada bagian Pusat Teknologi Informasi dan Komunikasi Perhubungan, serta Telkomsigma yang merupakan salah satu anak perusahaan dari PT. Telekomunikasi Indonesia. dan studi dokumen seperti buku, jurnal ilmiah, hasil-hasil keputusan, undang-undang dan peraturan pemerintah maupun sumber elektronik terpercaya.[10] Pengolahan dan pemeriksaan keabsahan data (triangulasi) menggunakan *software* NVivo 12 Plus serta dipertajam dengan analisis data menggunakan *Soft System Methodology* (SSM).

HASIL DAN PEMBAHASAN

Keamanan informasi dalam *cyber security* merupakan hal yang sangat penting. Hal ini dikarenakan pada umumnya penyerang mempunyai tujuan yang sama yaitu dapat mengakses informasi, bahkan mengendalikan informasi yang bersifat terbatas dan

[9] Agustinus Bandur, *Penelitian Kualitatif Metodologi, Desain, dan Teknik Analisis Data dengan NVIivo 11 Plus*, (Jakarta: Mitra Wacana Media, 2016), hlm.49-51.

[10] Agustinus, *loc. cit.,* hlm.109.

strategis. Oleh karena itu keamanan informasi mempunyai prinsip dasar yaitu *Confidentiality* (kerahasiaan) di mana informasi yang ada pada sistem/*data base* merupakan hal yang rahasia dan pengguna yang tidak berkepentingan tidak berhak mengaksesnya. Prinsip dasar kedua adalah *Integrity* (integritas) yang mempunyai arti data tidak dapat dirubah dari aslinya oleh orang yang tidak berhak, sehingga konsistensi, validitas, dan akurasi data tersebut masih terjaga. Kemudian prinsip dasar keamanan informasi yang terakhir adalah *Availability* (ketersediaan) yang berarti memastikan sumber daya akan selalu siap (*stand by*) dan siap diakses kapanpun dan dimanapun oleh user yang berhak. Faktor-faktor yang mempengaruhi *availability* dapat disebabkan oleh ketersengajaan seseorang/kelompok atau memang karena kecelakaan atau kejadian-kejadian alam seperti gempa bumi, kebakaran, dan lainnya.

Cyber security terbagi atas *cyber security* secara *software* maupun *hardware*, dan *cyber security awareness* yaitu *cyber security* yang lebih menitik beratkan kepada operator atau orang yang menjalankan *cyber security* secara sistem. Orang-orang yang berada dalam organisasi dapat memiliki peran kunci untuk menciptakan suasana strategi *cyber security* yang efektif dengan menggunakan kebijakan dan prosedur untuk menghindari serangan yang paling mendasar. Mengurangi resiko yang dibuat oleh manusia bukan hanya tentang meningkatkan peraturan dan pembatasan. Namun sebaliknya, pengembangan budaya keamanan yang efektif akan tergantung pada tingkat kesadaran dan pemahaman akan resiko dunia maya. Serta penanaman nilai-nilai dan perilaku "sadar keamanan" penting untuk dibina dalam organisasi tersebut.[11]

Implementasi keamanan informasi membutuhkan beberapa komponen seperti Keamanan Fisik dan Lingkungan, Keamanan Sumber Daya Manusia, Kebijakan Keamanan, Kontrol Akses, Manajemen Aset, Manajemen Komunikasi dan Operasi, Pengaturan tentang Keamanan Informasi, Pengembangan dan Pemeliharaan Akuisisi Sistem Informasi, dan Penilaian Resiko dan Perawatan.

[11] Anita Chandraker,"*How can you improve cyber security awareness in your organization*?", 2012, dalam https://www.paconsulting.com/insights.

Implementasi Sistem Keamanan Informasi Aplikasi Inaportnet

Inaportnet sebagai sistem aplikasi untuk layanan tunggal berbasis internet/web berperan untuk mengintegrasikan sistem informasi kepelabuhanan yang melayani kapal dan barang dari seluruh intansi atau pemangku kepentingan di pelabuhan. Inapornet bersifat terbuka dan netral oleh karena itu Inaportnet merupakan jalur lalu lintas informasi yang padat selain karena pelayanan di dalamnya banyak, juga karena aplikasi ini terhubung satu Indonesia. Tantangan dari penerapan Inaportnet di Indonesia adalah dukungan infrastruktur jaringan internet yang harus dibangun di setiap pelabuhan untuk mendukung kelancaran operasional Inaportnet.

Pembagian peran aplikasi Inapornet adalah sebagai berikut, Inaportnet berada dibawah tanggung jawab Direktorat Jenderal Perhubungan Laut. Untuk pengontrolan dan pengawasan dari aplikasi ini dilakukan oleh Direktorat Lalu Lintas dan Angkutan Laut, dan dibantu oleh Pusat Teknologi Informasi dan Komunikasi Perhubungan. Sedangkan untuk operasional pelayanan dari aplikasi Inaportnet diserahkan kepada masing-masing Unit Pelaksana Teknis di pelabuhan. Kemudian sistem pengamanan dari Aplikasi Inapornet ini dilakukan secara terpusat, termasuk penggunaan dan transmisi data/informasi didalamnya semuanya disimpan dalam *data base* terpusat yang dikelola oleh Telkomsigma.

Teknologi informasi dan komunikasi telah mencapai domain maritim di Indonesia, salah satunya adalah Inaportnet yang dalam pengoperasiannya berbasiskan kepada jaringan internet. Walaupun dapat dikatakan Inaportnet merupakan sebagian kecil bagian dari *maritime cyber* namun informasi yang berlalu lalang di dalam aplikasi ini sangat banyak. Kemudian data/informasi yang dimuat didalamnya juga bersifat penting. Oleh karena itu, menjadi sebuah kebutuhan aplikasi Inaportnet untuk melakukan tindakan pencegahan dalam menghadapi ancaman *cyber*.

Berdasarkan keterangan hasil wawancara dengan pihak Direktorat Lalu Lintas dan Angkutan Laut serta Pusat Teknologi Informasi dan Komunikasi Perhubungan tidak ada serangan *cyber* yang menyerang sistem Inaportnet hingga menyebabkan hal yang serius

terhadap aplikasi Inaportnet. Namun diakui adanya serangan yang dihadapi hanya serangan dengan level ringan, yakni serangan yang hanya menyerang sistem pengamanan luar dari Inaportnet itupun jarang frekuensinya. Menurut penelitian terdahulu yang dilakukan oleh Jenna Ahokas dan Tuomas Kiiski (2017) dalam tulisannya yang berjudul "*Cyber Security in Ports*" hal ini dikarenakan ancaman dalam *cyber security* dapat dicegah dan diminimalisir apabila sistem pengamanannya telah dipersiapkan secara maksimal, mulai dari jaringan, *hardware*, *software*, *virtual*, lingkungan, *data base*nya serta individunya. Juga berdasarkan teori *cyber security*, pertahanan terbaik dalam menjaga keamanan *cyber* adalah dengan melakukan pencegahan-pencegahan agar informasi di dalam sistem tetap aman.

Sistem pencegahan ini berguna untuk keamanan informasi dalam aplikasi Inaportnet. Meski prosedur pencegahan ini telah dilakukan oleh Telkomsigma sebagai pihak ketiga dalam penyedia dan pelaksana sistem pengamanan informasi Inaportnet. Namun, perlu juga untuk menumbuhkan *cyber security awareness* dalam tingkat individu karena pada dasarnya individu-individu ini merupakan pencegahan dari ancaman *cyber* yang efektif.

Cara – cara yang menunjukkan hubungan antara langkah-langkah teknis, perilaku karyawan dan tindakan organisasi baik selama maupun diluar jam kerja dapat meningkatkan lingkungan kerja yang aman. Beberapa pendekatan yang dapat untuk meningkatkan kesadaran *cyber security* adalah eksplorasi yaitu dengan memutar ulang suatu kejadian, sehingga orang-orang dapat mencapai solusi konstruktif yang disepakati bersama. Kedua yaitu Kesadaran yaitu dengan mengalami sendiri bagaimana suatu situasi dapat berubah, dan para pemangku kepentingan dapat melihat dampak dari kebijakan dan peraturan mereka. Ketiga, Perubahan Perilaku dengan cara mengalami dan merefleksikan suatu situasi, sehingga orang akan sadar terkait perilakunya dan memiliki kesempatan untuk menghadapinya dengan perilaku yang berbeda dan lebih tepat sasaran. Keempat adalah pelatihan dengan mengadakan pelatihan maka orang-orang dapat dengan aman bereksperimen, melakukan kesalahan, dan belajar sekaligus melakukan.

Aspek Keamanan Informasi Aplikasi Inaportnet

Berdasarkan teori keamanan informasi terdapat aspek dasar keamanan informasi harus memenuhi 3 kriteria yaitu Keamanan informasi bertujuan untuk memastikan bahwa informasi yang sensitive hanya dapat diinformasikan kepada pihak yang berwenang (*confidentiality*), mencegah modifikasi data yang tidak sah (*integrity*), dan menjamin data dapat diakses oleh pihak yang berwenang ketika dibutuhkan (*availability*). Aspek ini dapat dicapai ketika implementasi sistem keamanan informasi diterapkan secara maksimal.

Dalam implementasi keamanan informasi juga terdapat sembilan komponen yang akan mendukung tercapainya ketiga aspek dasar keamanan informasi tersebut. Pelaksanaan sembilan komponen tersebut telah terpenuhi dengan baik dalam aplikasi Inaportnet. Sehingga ketiga aspek tersebut juga telah terpenuhi. Ke-sembilan komponen ini mencakup seluruh implementasi keamanan informasi dalam aplikasi Inaportnet. Mulai dari keamanan dari segi informasi itu sendiri, lingkungan baik fisik maupun virtual, keamanan *hardware* dan *software*, pembagian hak akses, perlindungan terhadap informasi jaringan serta pembagian level informasi.

Menurut John R.Vacca (2009) ketiga aspek dasar keamanan informasi yang pertama integritas yaitu dengan mengaplikasikan beberapa teknologi seperti enkripsi, authentikasi dan validasi yang kuat, pembatasan dan pembagian akses kontrol yang jelas. Kedua adalah ketersediaan yaitu dengan memastikan beberapa hal seperti *Disaster Recovery Plan*, Tenaga Cadangan untuk sumber listrik, RAID (*Redundant Array of Independent Disks*), serta data *backup*. Ketiga adalah kerahasiaan hal yang dapat dipastikan adalah enkripsi saat transmisi data dan kekuatan *password*. Berdasarkan ketentuan tersebut dapat disimpulkan bahwa aspek keamanan informasi dalam aplikasi Inaportnet telah terpenuhi.

Walaupun aspek dasar keamanan informasi telah terpenuhi, terdapat satu hal yang dapat menyempurnakan keamanan informasi dalam aplikasi Inaportnet, yaitu apabila aplikasi ini mempunyai *Information Security Handbook for Inaportnet. Handbook* ini juga sering disebut sebagai *standard*, *guideline* atau *guidance*. Hal ini dilakukan

untuk mengatur hal-hal penting yang berkaitan dengan segala kegiatan dan kebijakan untuk mendukung terwujudnya keamanan informasi dalam aplikasi Inaportnet yang maksimal.

Menurut Timothy P. Layton (2007) *handbook* untuk keamanan informasi digunakan sebagai dokumen untuk kontrol kebijakan keamanan informasi dengan penunjukkan persyaratan yang jelas dalam pengembangan dan penerbitan dokumen kebijakan keamanan informasi. Dokumen ini juga dapat menjadi kontrol untuk penekanan pentingnya mengkomunikasikan kebijakan kepada semua pihak secara tepat termasuk karyawan, pihak eksternal, dan organisasi lain yang termasuk didalamnya. Kode praktik tidak memberikan panduan khusus bagaimana mencapai hal ini, tetapi menyarankan kebijakan yang dikomunikasikan secara efektif akan mendapatkan penerimaan dan kepatuhan pengguna target.

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dijelaskan pada Bab satu hingga empat serta ditambah dengan analisa SSM, maka dapat ditarik kesimpulan yang menjawab rumusan masalah pada penelitian ini yaitu sebagai berikut:

a. Implementasi sistem keamanan informasi Inaportnet di lapangan sudah berjalan dengan baik namun belum berjalan secara efektif dan efisien. Hal ini dikarenakan salah satu aspek pendukung sistem keamanan informasi yang juga penting yaitu kesadaran tentang pentingnya keamanan informasi (*awareness*) dapat dikatakan masih kurang. Hal ini dibuktikan dengan temuan dilapangan yaitu tidak adanya jadwal rutin untuk kegiatan *penetration test* dan *patch*. Jadwal secara rutin untuk *penetration test* dan *patch* selain untuk mengetahui kelemahan-kelemahan dalam sistem pengamanan informasi di Inaportnet juga untuk meminimalisir ancaman *cyber* yang dapat berevolusi setiap waktu.
b. Keamanan informasi dalam aplikasi Inaportnet belum dijadikan sebagai salah satu prioritas oleh Direktorat Lalu Lintas dan Angkutan Laut. Hal ini berdasarkan temuan di lapangan yang kemudian diolah dalam analisa. Hal ini juga dibuktikan dengan tidak adanya Inaportnet *Information Security*

Handbook untuk para pemangku kepentingan dalam kegiatan kepelabuhanan. Handbook ini tidak hanya berfungsi sebagai *standard* atau *guidance* bagi para pemangku kepentingan dalam aplikasi Inaportnet akan tetapi *handbook* ini juga sebagai representatif kebijakan-kebijakan keamanan informasi yang diimplementasikan dalam aplikasi Inaportnet.

REKOMENDASI

Peneliti memberikan rekomendasi yang didapat dari hasil penelitian ini. Rekomendasi ini diajukan sesuai dengan permasalahan yang muncul pada latar belakang penelitian dengan harapan isu yang diangkat dalam penelitian ini dapat dijadikan bahan pertimbangan oleh pihak-pihak yang berkepentingan dalam aplikasi Inaportnet, serta secara akademis dapat dilanjutkan dalam penelitian selanjutnya.

Rekomendasi Teoritis

Di dalam penelitian ini telah dibuktikan bahwa teori implementasi, teori keamanan nasional, konsep keamanan maritim, teori *cyber security*, dan teori keamanan informasi dapat digunakan dalam penelitian terkait dengan implementasi sistem pengamanan informasi dalam aplikasi Inaportnet untuk mendukung *maritime cyber security*. Penggunaan SSM dan NVivo sangat membantu dalam penelitian ini, sehingga dapat menghasilkan analisa yang tajam serta terstruktur. Metode ini direkomendasikan untuk digunakan dalam penelitian kualitatif lainnya. *Gap* yang ditemukan dalam penelitian ini dalam perbandingan model konseptual dengan realitas dapat dikembangkan menjadi penelitian lebih lanjut. Pembahasan yang dapat diambil diantaranya adalah *cyber security awareness* dalam aplikasi Inaportnet, penelitian lebih lanjut tentang efektifitas adanya *informasi security handbook* dalam aplikasi Inaportnet.

Rekomendasi Praktis

Berdasarkan hasil dari *Root Definition* dalam penelitian ini maka dapat pula ditarik beberapa saran teoritis terhadap owners.

Rekomendasi praktis yang pertama ditujukan kepada Direktorat Jenderal Perhubungan Laut sebagai penanggung jawab aplikasi Inaportnet. Hal yang direkomendasikan berupa pembuatan Inaportnet *Information Security Handbook* yang dibuat khusus untuk para pemangku kepentingan di

pelabuhan. *Handbook* ini akan berisi siapa saja yang bertanggung jawab, pengkategorian level informasi, siapa dan apa yang dapat mengakses informasi dalam inaportnet (akses kontrol), manual prosedur yang digunakan ketika terjadi *error/trouble*, pembatasan akses, teknis perlindungan informasi, *monitoring*, audit, *self-assesment*, hingga materi pelatihan tentang pengetahuan dan kesadaran akan pentingnya keamanan informasi.

DAFTAR PUSTAKA

Buku

Kementerian Pertahanan Republik Indonesia. 2015. *Buku Putih Pertahanan Indonesia*. Jakarta: Kementerian Pertahanan Indonesia.

Layton, Timothy P. 2007. *Informaton Security: Design, Implementation, Measurement, and Compliance*. Florida: Auerbach Publications, Taylor & Francis Group.

Vacca, John R. 2009. *Computer and Information Security Handbook*. USA: Morgan Kaufmann Publishers imprint of Elsevier.

Bandur, Agustinus. 2016. *Penelitian Kualitatif: Metodologi, Desain, dan Teknik Analisis Data dengan NVIVO 11 plus*. Jakarta: Mitra Wacana Media.

Springer, Paul J. 2013. *Cyber Warfare: a reference handbook*. USA : ABC-CLIO, LLC.

Jurnal

Darmono, Bambang. 2010. "Konsep dan Sistem Keamanan Nasional Indonesia". *Jurnal Ketahanan Nasional*. Volume 15 (1).

Bueger, Christian. 2014. "What is *Maritime* Security?". *Marine Policy*, Volume 53.

Grozdanoska, Natasha.2014. "National Defence and Security". *European Scientific Journal*. Volume.1. ISSN-1857-7431.

Ahokas, Jenna dan Tuomas Kiiski. 2017. "*Cybersecurity*in Ports". *Publication of the Hazard Project*: Volume 3.

Peraturan

Peraturan Menteri Perhubungan Nomor 192 Tahun 2015 tentang perubahan atas PM Nomor 157

Tahun 2015 tentang Penerapan Inaportnet untuk Pelayanan Kapal dan Barang di Pelabuhan.

Website

Anita Chandraker,"*How can you improve cyber security awareness in your organization*?" dalam https://www.paconsulting.com/insights/how-can-you-improve-*cyber*-security-awareness-in-your-organisation/ diakses pada 27 November 2018.