MEMBANGUN KEWASPADAAN KEAMANAN SIBER TNI AL SEBAGAI BAGIAN STRATEGI PERTAHANAN LAUT INDONESIA

BUILDING NAVY CYBERSECURITY VIGILANCE AS PART OF INDONESIA'S SEA DEFENSE STRATEGY

Syaeful Bakhri[1], Lukman Yudho Prakoso[2], Aries Sudiarso[3]

STRATEGI PERTAHANAN LAUT FAKULTAS STRATEGI PERTAHANAN
UNVERSITAS PERTAHANAN RI
(siipul80@gmail.com**,** lukman.prakoso@outlook.com, aries.25st@yahoo.co.id)

Abstrak-Perkembangan kemajuan teknologi informatika dalam dunia siber saat ini, telah banyak membuat perubahan terhadap kehidupan sosial manusia. Yang memiliki dampak positif dan negatif sebagai konsekuensinya, dampak negatif tersebut adalah kejahatan siber yang berupa serangan-serangan lewat jaring komunikasi dan data yang mengakibatkan gangguan terhadap sistem sosial yang bisa mengancam keamanan dan pertahanan bangsa. Serangan yang dimaksud dapat datang *state* dan *non state actor*, ancaman ini semakin meningkat eskalasinya akhir-akhir ini sehingga memerlukan perhatian khusus untuk mengatasinya dengan bijak. TNI AL sebagai komponen utama dalam Startegi Pertahanan Laut juga tidak luput dari ancaman siber ini, oleh karena tujuan dari serangan siber adalah data atau informasi yang bisa disalah gunakan oleh para *Hacker*, hal ini dapat dicegah atau diminimalisir dengan cara membangun kewaspadaan keamanan siber terhadap data dan informasi secara umum agar terjaga dari para hacker, yang dimulai dari kewaspadaan personal TNI AL, terutama yang mengelola data dan informasi penting/krusial. Metodelogi yang digunakan pada artikel ini adalah studi pustaka dengan pendekatan teori komunikasi dan pertahanan siber dengan literatur peraturan kementerian pertahanan yang memberikan pedoman penanganan pertahanan siber, untuk mencari solusi terhadap ancaman dan serangan siber dengan cara membangun kewaspadaan keamanan siber pada personel TNI AL. Dengan mempelajari kemungkinan datangnya serangan dan celah-celah dalam sistem yang dapat menjadi kelemanan yang digunakan oleh *hacker* maka dapat diambil simpulan adalah Sebagian besar serangan adalah dari *human error* yang kurang waspada terhadap keamanan data dan informasi krusial baik pribadi ataupun organisasi. Dengan mengambil contoh kasus serangan siber selama tahun 2019.

Kata Kunci: Data, Kewaspadaan siber, Pertahanan siber, Serangan siber, Teknologi Informasi.

Abstract-The development of advances in informatics technology in today's cyber world has made many changes to human social life. Which has a positive and negative impact as a consequence, the negative impact is a cybercrime in the form of attacks through the net of communication and data that cause disruption. against social systems that could threaten the security and defense of the nation. The attacks in question can come from state and non-state actors, this threat is increasingly escalating lately so it requires special attention to deal with it wisely. Indonesian Navy as the main component in the Sea Defense Strategy is also not spared from this cyber threat, because the purpose of cyberattacks is data or information that is Can be misused by hackers, this can be prevented or minimized by building cybersecurity awareness of data and information in general. To be awake from hackers starts from the personal vigilance of the Navy, especially those who manage important/crucial data and information. The methodology used in this article is a literature study with a communication theory and cyber defense approach with the ministry's regulatory literature defense that provides guidelines for handling cyber defense, to find solutions to threats and cyberattacks by establishing cybersecurity vigilance on navy personnel. By studying the possibility of attacks and gaps in the system that can be a slowness used by hackers, it can be taken into conclusion. Large attacks are from human errors that are less alert

to the security of data and crucial information both personal and organizational. By taking the example of a cyber attack during 2019.

Keywords: *Cyberattacks, Cyberdefense, cyber vigilance, Data, Technology Information Technology.*

Pendahuluhan

Dengan semakin berkembangnya teknologi infomasi dan digital saat ini, yang sudah menyebar ke semua aspek kehidupan sangat membantu peradaban dan kehidupan manusia. Dalam hal hubungan dan pertukaran informasi yang sudah tidak mengenal batas ruang dan waktu, hal ini secara signifikan meningkatkan kualitas kehidupan, baik kehidupan manusia sebagai individu dan manusia dalam komuniti sosial bernegara.

Namun selain manfaatnya tersebut secara logis pasti terdapat dampak negatifnya yang berupa ancaman-ancaman terhadap pertukaran informasi yang saat ini sangat umum dan cepat, dengan munculnya *Hacker* yang merentas dan mengakibatkan gangguan pada sistem pelayanan public serta pencurian data-data sensitive ataupun rahasia.

Ancaman siber yang ada saat ini terjadi oleh karena banyak faktor salah satunya adalah kesalahan manusia (*Human error*) yang terjadi akibat kurang pedulinya terhadap keamanan data/informasi, kaitannya dalam penggunaan teknologi informasi yang saat ini sudah menjadi bagian dari kehidupan.

Dengan menganalisa perkembangan budaya kerja, dan informasi ancaman dan serangan siber yang ada, adalah kemungkinan *human error* ini harus diminimalisir. Dalam militer secara khusus TNI AL juga tidak terhidar dari permasalahan ancaman dan serangan siber, oleh karena itu perlu adanya usaha-usaha untuk membangun kewaspadaan terhadap keamanan siber sebagai bagian dari strategi pertahanan laut Indonesia.

Metode penelitian

Dalam artikel ini metode penelitian dilakukan dengan menggunakan metode penelitian kualitatif, dengan pengumpulan dan analisis data (teks, video, audio) untuk memahami konsep, pendapat, atau pengalaman. Ini dapat digunakan untuk mengumpulkan informasi mendalam tentang suatu masalah atau menghasilkan konsep baru untuk penelitian. Setiap pendekatan penelitian melibatkan penggunaan satu

atau lebih metode pengumpulan data. Pada penelitian ini, peneliti menggunakan penelitian sekunder dengan mengumpulkan data yang ada berupa teks, gambar, video, dll. Serta studi pustaka dari beberapa buku dan artikel BSSN, para ahli siber nasional dan internasional.

Hasil dan Pembahasan.

Perlunya usaha-usaha membangun kewaspadaan keamanan siber di TNI AL baik sumber daya manusia dan infrastruktur nya adalah suatu Langkah yang urgen, terkait siber dari perspektif komunikasi "*the heralding of a second media age is almost exclusively based on the rise of interactive media, most especially the Internet*" (David Holmes. 2005). Siber menjadi salah satu media komunikasi interaktif lewat internet, yang memang sudah digunakan menjadi domain dalam teknologi dan aktifitas kerja TNI AL.

Oleh karena itu TNI AL yang menjadi kekuatan utama dalam strategi pertahanan laut, juga memiliki resiko ancaman dan serangan siber yang dapat mengakibatkan ganguan terhadap komunikasi serta infrastuktur sibernya.

Untuk memulai pembahasan artikel ini mencantumkan dalam Peraturan Menteri Pertahanan Republik Indonesia, Nomor 82 Tahun 2014, Tentang Pedoman Pertahanan Siber. Yang berisi tentang pedoman dan penjelasan konsep umum pertahanan siber Indonesia oleh Lembaga serta kementerian negara. Lebih lanjut akan dibahas dalam pembahasan secara literatur dan komprahensif pada kajian berikut.

Ruang siber

Ruang siber (*Cyberspace*) adalah ruang dimana komunitas saling terhubung menggunakan jaringan yaitu internet untuk melakukan berbagai kegiatan sehari-hari. Ruang siber merupakan wilayah yang berkaitan erat dengan "penggunaan alat elektronik dan spektrum elektromagnetik untuk menyimpan, mengubah, atau bertukar informasi sampai lingkup global, melalui sistem informasi jaringan dan infrastruktur fisik yang mendukungnya" (Kuehl, D., & Pudas, T., 2010). Wilayah ini memiliki karakter yang unik karena meski tetap memerlukan teknologi, tetapi tidak lagi hanya mengandalkan ruang fisik sebagaimana darat dan laut. Oleh karena itu di dalam ruang siber ada peluang untuk mengeksploitasi informasi, interaksi manusia, dan interkomunikasi. Dengan tiga unsur penting itu, ruang

siber menyimpan potensi sebagai sumber kekuatan siber (*Siberpower*) bagi pihak pengguna, baik itu individu, organisasi, maupun negara.

Istilah "ruang siber" digunakan pada buku karya Werner J Severin dan James W Tankard Jr yang *berjudul Communication Theorie: Origins, Methods, & Uses in the Mass Media,* dan kemudian ruang siber (*Cyberspace*) di populerkan oleh penulis fiksi ilmiah William Gibson dalam bukunya yang berjudul *Neuromencer*, sehingga menjadi istilah yang sering digunakan untuk merujuk pada ranah metaforis komunikasi elektronik, dimana ruang siber yang menjadi tempat interaksi.

"A theory of communication must be developed in the realm of abstraction. Given that physics has taken this step in the theory of relativity and quantum mechanics, abstraction should not be in itself an objection" (D. Holmes, 2005). Menurut D. Holmes objek ruang siber tidak terbatas dalam ruang fisik dalam kontek abstraksinya. Sehingga semua kejadian didalam ruang siber tidak terbatas oleh ruang fisik dan waktu, interaksi dan komunikasi dapat dilakukan dengan cepat serta seketika, oleh perorangan atau organisasi dengan efektif dan praktis tidak dapat dilaksanakan.

Gibson menjelaskan Ruang Siber adalah, *A consensual hallucination experienced daily by millions of legitimate operators. A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the no space of the mind, clusters, and constellations of data. Like city lights, receding*. (Gibson, 1984).

Keamanan siber.

Keamanan Siber Nasional (*National siber security*) adalah segala upaya dalam rangka menjaga kerahasiaan, keutuhan dan ketersediaan informasi serta seluruh sarana pendukungnya di tingkat nasional, yang bersifat lintas sektor. Yang ditujukan untuk perlindungan terhadap serangan siber.

Undang-Undang RI Nomor 3 Tahun 2002 tentang Pertahanan Negara. Menyebutkan bahwa pertahanan negara bertujuan untuk menjaga dan melindungi kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia (NKRI) dan keselamatan segenap bangsa dari segala bentuk ancaman, baik ancaman militer maupun non-militer.

Ancaman non militer khususnya di ruang siber telah menyebabkan kemampuan negara dalam bidang *soft* dan *smart power* pertahanan harus ditingkatkan melalui strategi penangkalan, penindakan dan pemulihan pertahanan siber (*Cyber defense*) dalam rangka mendukung penerapan strategi nasional keamanan siber yang dimotori oleh Kementerian Komunikasi dan Informatika. Lebih lanjut keamanan siber telah menjadi disiplin multi domain horizontal yang mencakup banyak bidang dan pendekatan. Memang, karena hubungan antara berbagai aspek kehidupan digital dan fisik kita, konsep keamanan siber melibatkan pengetahuan yang berasal dari berbagai disiplin ilmu yang berbeda, dan kadang-kadang sangat jauh (Komisi Eropa dan Direktorat Jenderal Untuk Penelitian dan Inovasi, 2017).

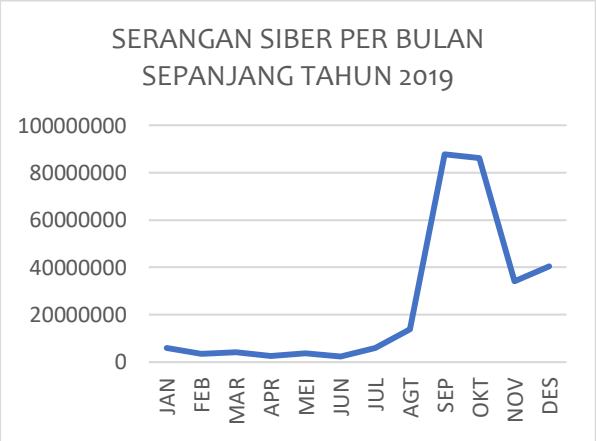
Serangan Siber.

Serangan Siber adalah segala bentuk perbuatan, perkataan, pemikiran baik yang dilakukan dengan sengaja maupun tidak sengaja oleh pihak mana pun, dengan motif dan tujuan apa pun, yang dilakukan di lokasi mana pun, yang disasarkan pada sistem elektronik atau muatannya (informasi) maupun peralatan yang sangat bergantung pada teknologi dan jaringan dalam skala apa pun, terhadap obyek vital maupun nonvital dalam lingkup militer dan nonmiliter, yang mengancam kedaulatan negara, keutuhan wilayah dan keselamatan bangsa.

Adapun beberapa kejadian terkait serangan siber beberapa diantaranya adalah skandal pencurian data Facebook untuk kampanye pemilu Donald Trump. Masyarakat Indonesia dan dunia juga sempat disibukkan dengan isu penyalahgunaan data pribadi oleh *FaceApp*.

Serangan Siber yang menyasar ke Indonesia selama periode Januari hingga November 2020 mencapai 423 juta kali. Angka tersebut berdasarkan Data Badan Siber dan Sandi Negara (BSSN) tahun 2019. Jumlah tersebut naik tiga kali lipat dibandingkan periode sama pada tahun lalu. Data statistik tersebut perlu menjadi perhatian bagi pengguna internet di Indonesia. Sebab serangan siber tak melulu hanya berkaitan pada perangkat keras atau perangkat lunak semata. Kepala Badan Siber dan Sandi Negara (BSSN) Hinsa Siburian menyatakan, serangan tersebut terbagi dalam dua sifat, yaitu serangan sosial dan teknis. Serangan sosial berupa upaya untuk

mempengaruhi manusia pada dan melalui ruang siber dan cenderung berkaitan erat dengan perang politik, perang informasi, perang psikologi, dan propaganda.



Gambar 1 serangan siber 2019
Sumber: Mata Garuda - IDSIRTII, 2019

Jenis Ancaman.

Jenis Ancaman Menurut Michael D. Mcdonnell dan Terry L. Sayers, jenis ancaman siber dikelompokkan dalam:

1. Ancaman Perangkat Keras (*hardware threat*), yaitu ancaman yang disebabkan oleh pemasangan peralatan tertentu yang berfungsi untuk melakukan kegiatan tertentu dalam suatu sistem, sehingga peralatan tsb merupakan gangguan terhadap sistem Jaringan dan Perangkat Keras lainnya, contoh: *Jamming* dan *Network Intrusion*.
2. Ancaman Perangkat Lunak (*software threat*), yaitu ancaman yang disebabkan oleh masuknya *software* tertentu yang berfungsi untuk melakukan kegiatan seperti: Pencurian Informasi (*Information Theft*), Perusakan Informasi/Sistem (*Information/System Destruction*), Manipulasi Informasi (*Information Corruption*) dan lain sebagainya, ke dalam suatu sistem.
3. Ancaman Data/Informasi (*data/information threat*), adalah ancaman yang diakibatkan oleh penyebaran data/informasi tertentu yang bertujuan untuk kepentingan tertentu, seperti yang dilakukan dalam *information warfare* termasuk kegiatan propaganda.

Bentuk Ancaman

Berdasarkan Permenhan No. 82 Tahun 2014 tentang Pedoman Pertahanan Siber, bentuk ancaman siber yang sering terjadi saat ini dapat berupa hal-hal sebagai berikut:

1. Serangan *Advanced Persistent Threats* (APT), *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS), biasanya dilakukan dengan melakukan *overloading* kapasitas sistem dan mencegah pengguna yang sah untuk mengakses dan menggunakan sistem atau sumber daya yang ditargetkan. Serangan ini bertujuan

untuk mengganggu operasional sistem, dengan cara menghadapkan sistem pada permintaan akses dan proses yang jauh lebih besar dari yang bisa ditangani sistem. Sehingga sistem menjadi terlalu sibuk dan *crash*, akibatnya menjadi tidak dapat melayani atau tidak dapat beroperasi. Permasalahan ini merupakan ancaman yang berbahaya bagi organisasi yang mengandalkan hampir sepenuhnya pada kemampuan internet guna menjalankan roda kegiatannya.

2. Serangan *Defacement*, dilakukan dengan cara melakukan penggantian atau modifikasi terhadap halaman web korban sehingga isi dari halaman web korban berubah sesuai dengan motif penyerang.
3. Serangan *Phishing*, dilakukan dengan cara memberikan alamat *website* palsu dengan tampilan persis sama dengan website aslinya. Tujuan dari serangan *phishing* ini adalah untuk mendapatkan informasi penting dan sensitif seperti *username*, *password* dan lain-lain.
4. Serangan *Malware*, yaitu suatu program atau kode berbahaya yang dapat digunakan untuk mengganggu operasi normal dari sebuah sistem komputer. Biasanya program *malware* telah dirancang untuk mendapatkan keuntungan finansial atau keuntungan lain yang direncanakan. Jumlah serangan *malware* terus berkembang, sehingga saat ini telah menjadi pandemi yang sangat nyata. *Malware* telah terjadi dimana-mana dan mempengaruhi semua orang yang terlibat dalam setiap sektor kegiatan. Istilah virus generik digunakan untuk merujuk setiap program komputer berbahaya yang mampu mereproduksi dan menyebarkan dirinya sendiri.
5. Penyusupan siber, yang dapat menyerang sistem melalui identifikasi pengguna yang sah dan parameter koneksi seperti *password*, melalui eksploitasi kerentanan yang ada pada sistem. Metode utama yang digunakan untuk mendapatkan akses ke dalam sistem adalah:
   a. Menebak. Sandi yang begitu jelas, seperti nama pengguna, nama pasangan atau anak, tanggal lahir atau berbagai hal yang penting yang berkaitan

dengan diri dan keluarganya, sangat mudah untuk ditebak dan dipecahkan. *Account* yang tidak terlindungi. Pengguna juga dapat melakukan kesalahan, dengan tidak memasang *password* atau dengan mudah memberikan *password* kepada orang lain.

b. Penipuan dan Rekayasa Sosial, misalnya pelaku dapat mengaku dan bertindak sebagai *administrator* dan meminta *password* dengan beberapa alasan teknis. Dalam sejumlah besar kasus, pengguna akan mengungkapkan data mereka. Pelaku dapat menipu melalui telepon atau pesan elektronik. Beberapa orang pelaku tidak faham komputer, tetapi ternyata pelaku dapat memperoleh kunci sesuai dengan sistem yang mereka inginkan untuk ditembus.

c. Mendengarkan lalu lintas komunikasi data. Penyadap akan mendengarkan data yang tidak terenkripsi yang dikirimkan melalui jaringan melalui protokol komunikasi. Mereka beroperasi menggunakan PC dengan cara mengendus (*sniffing*) dan menganalisis data dalam transit di jaringan, kemudian mengekstraksi *password* terenkripsi yang ditularkan oleh pengguna selama koneksi. Jika pelaku tidak bisa mengandalkan keterlibatan dari dalam organisasi dalam mendapatkan *password* secara langsung, maka dengan bantuan perangkat elektronik mereka dapat mencegatnya dari protokol komunikasi atau mengakses file yang berisi semua *password*.

d. *Trojan Horse*. Program mata-mata yang spesifik dan sangat berbahaya (*spyware*) secara diam-diam dapat merekam parameter yang digunakan untuk menghubungkannya ke sistem *remote*. *Trojan* adalah sebuah program kecil yang umumnya pengganti dirinya untuk kode login yang meminta pengguna untuk menangkap atau memberikan identifikasi dan *password*, dengan keyakinan bahwa ia berada dalam lingkungan operasi normal, dimana sandi segera ditransmisikan ke server sebagai pesan anonim dari pelaku.

e. Sistem Otentifikasi. Semua *password* pengguna harus disimpan pada sebuah server. Pelaku akan mengakses file yang menyimpan semua *password user* yang dienkripsi, untuk kemudian dibuka dengan utilitas yang tersedia pada jaringan.

f. *Cracking Password* Terenkripsi. Jika pelaku atau *cracker* tahu algoritma *cypher*, ia bisa menguji semua permutasi yang mungkin, yang dapat merupakan kunci untuk memecahkan *password*. Serangan ini dikenal sebagai *brute force*. Alternatif lain adalah dengan menggunakan kamus untuk menemukan *password* terenkripsi, yang disebut serangan kamus. Dengan perbandingan berturut-turut, bentuk kode *password* yang terdapat dalam kamus kriminal dapat digunakan untuk menebak *password* terenkripsi yang digunakan.

g. Memata-matai. Hal ini dilakukan dengan merekam parameter koneksi mereka dengan menggunakan *software*, *spyware* atau perangkat multimedia, seperti kamera video dan mikrofon, guna menangkap informasi rahasia, seperti *password* untuk mengakses sistem yang dilindungi.

6. Spam, adalah pengiriman *Email* secara massal yang tidak dikehendaki, dengan tujuan:
   a. Komersial atau publisitas.
   b. Memperkenalkan perangkat lunak berbahaya, seperti *malware* dan *crimeware* ke dalam sistem.
   c. Pada situasi terburuk, spam menyerupai serangan bom *Email*, dengan akibat *mail server* mengalami kelebihan beban, *mailbox user* penuh dan ketidaknyamanan dalam pengelolaan. Sebelumnya *spam* hanya dianggap sebagai gangguan, tapi saat ini *Emailspam* merupakan ancaman nyata. Hal tersebut telah menjadi vektor istimewa untuk penyebaran virus, *worm, trojans, spyware* dan upaya *phishing*.

7. Penyalahgunaan Protokol Komunikasi. Sebuah serangan spoofing *Transmision Control Protocol* (TCP) bergantung pada kenyataan bahwa protokol TCP menetapkan koneksi logis antara

dua ujung sistem untuk mendukung pertukaran data. Pengidentifikasi logis (nomor port) digunakan untuk membangun sebuah koneksi TCP. Sebuah serangan TCP nomor port akan melibatkan kegiatan menebak atau memprediksi nomor port berikutnya yang akan dialokasikan untuk pertukaran data dalam rangka menggunakan angka-angka bukan pengguna yang sah. Hal ini memungkinkan untuk melewati firewall dan mendirikan sebuah hubungan yang aman antara dua entitas, yaitu hacker dan target.

Dampak Serangan Siber.

Berdasarkan Permenhan No. 82 Tahun 2014 tentang Pedoman Pertahanan Siber, dampak yang mungkin terjadi dari sebuah serangan siber dapat berbentuk:

1. Gangguan fungsional.
2. Pengendalian sistem secara *remote*.
3. Penyalahgunaan informasi.
4. Kerusuhan, ketakutan, kekerasan, kekacauan, konflik.
5. Serta kondisi lain yang sangat merugikan, sehingga memungkinkan dapat mengakibatkan kehancuran. (Menhan RI, 2014)

Sementara, serangan teknis lebih ditujukan menyerang jaringan logika melalui berbagi metode untuk mendapatkan akses ilegal, mencuri informasi, atau memasukkan *malware* yang bisa merusak jaringan fisik dan personal siber (pengguna internet). Serangan siber dapat bersifat teknis maupun sosial tergantung dari konteks bagaimana serangan tersebut dimaksud. Kepala BSSN Hinsa *talkshow* daring *#SiberCorner* bertajuk Ekosistem Ruang Siber Indonesia, mengatakan "Serangan siber dapat dikategorikan menjadi kriminal biasa, kriminal luar biasa dan perang siber bergantung dari tujuan dan intensitas serangan tersebut tanpa terbatas pada pembagian spektrum waktu dimasa damai, krisis atau dalam keadaan perang" baru-baru ini. Acara ini digagas oleh BSSN bersama Siberthreat.id.

Implementasi Kebijakan

Pemerintah melalui Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN) dan peraturan perubahannya Peraturan Presiden Nomor 133 Tahun 2017 membentuk BSSN yang bertugas melaksanakan keamanan siber secara efektif dan efisien dengan

memanfaatkan, mengembangkan dan mengkonsolidasikan semua unsur yang terkait dengan keamanan siber nasional.

Dan Peraturan Menteri Pertahanan Republik Indonesia, Nomor 82 Tahun 2014, Tentang Pedoman Pertahanan Siber. Pada poin 2.4 Kebutuhan Pertahanan Siber Kementerian Pertahanan dan Tentara Nasional Indonesia memiliki dua kepentingan dalam pertahanan siber. Pertama, untuk mengamankan semua sistem elektronik dan jaringan informasi di lingkungannya. Kedua, mendukung koordinasi pengamanan siber di sektor-sektor lainnya sesuai kebutuhan. Yang di wujudkan dengan di bentuknya Pushan Siber, Satsiber TNI, Labpamsisjar TNI AL, merupakan implementasi strategi pertahanan siber saat ini.

Laporan keamanan siber BSSN Tahun 2019.

Dunia siber Indonesia di tahun 2019 diramaikan dengan dua peristiwa besar. Peristiwa pertama terkait insiden siber yang terus menerus menghantam sistem keamanan siber nasional dan peristiwa kedua terkait usaha-usaha pemerintah memperkuat kemanan siber nasional itu sendiri. Karena serangan bisa datang dari mana saja bukan hanya dari Indonesia. Serangan siber juga belum tentu dilakukan dari sumber serangan yang tercatat tapi mungkin saja dari negara lain yang menjadikan negara sumber serangan itu sebagai pijakan atau platform saja. Sistem monitoring nasional mata garuda BSSN misalnya mencatat sebanyak 290,3 juta serangan siber yang masuk ke Indonesia sepanjang tahun 2019 ini serangan terbesar datang dari IP address berlokasi di Amerika Serikat, bergeser dari kondisi tahun sebelumnya yang tercatat lebih banyak dari IP address yang ada di Indonesia sendiri (BSSN, 2019).

Metode penyerangan siber menggunakan *malware* tercatat paling banyak digunakan didunia siber global, *hackmagedon* mencatat 39% dari top distribusi serangan siber dunia merupakan serangan menggunakan *malware*. Serangan *malware* masih menduduki peringkat pertama dalam serangan siber secara global. Tren yang sama diperlihatkan juga di Indonesia, *malware* menduduki peringkat pertama metoda serangan yang sering digunakan dalam sembilan bulan dari dua belas bulan sepanjang tahun 2019. 36,2% dari top distribusi serangan siber ke Indonesia tercatat merupakan serangan menggunakan *malware*.

Beberapa insiden siber penting lain selain malware adalah insiden kebocoran data dan *electricity blackout*. Insiden kebocoran data antara lain insiden kebocoran data penumpang yang terjadi pada Malindo Air yaitu anak perusahaan Lion Air, dan kebocoran data 13 juta akun Bukalapak yang diperjual belikan di situs dark web. Insiden *electricity blackout* (padamnya listrik) terjadi pada tgl 4 Agusttus 2019 selama 9 jam menimbulkan dampak yang besar terhadap jaringan internet dan bisnis digital yang berjalan diatasnya.

Tabel 1 Kejadian Keamanan Siber 2019

KEJADIAN PENTING KEAMANAN SIBER INDONESIA THN 2019	
TANGGAL	KEJADIAN KEAMANAN
18 Mar 2019	Kebocoran data 13 juta pengguna Bukalapak
24 May 2019	Pembatasan media sosial Whatsapp oleh Kemeninfo
18 Sept 2019	Kebocoran 7,8 juta data pribadi penumpang Malindo Air
22 Sept 2019	Website Kemendagri di retas
24 Sept 2019	Website DPR tidak bisa diakses
25 Sept 2019	Website KPAI di retas
15 Oct 2019	Website BMKG di retas
19 Des 2019	Website Pengadilan Negeri Jakarta Pusat di retas
28 Des 2019	Website Bareskrim Polri di retas
30 Des 2019	Website Bawaslu Jakarta Pusat di retas

Sumber: BSSN, 2019

Ancaman siber akan terus ada dan semakin canggih. Bukan hanya di Indonesia, negara Amerika pun mengalami kesulitan menghadapi ancaman ini. Menurut FBI, tindakan kriminal siber di Amerika sepanjang tahun 2019 telah mengakibatkan kerugian 3,5 Milyar dolar atau sekitar 47,9 trilyun rupiah. Donna Gregory, kepala Pusat Aduan Kejahatan Internet FBI mengatakan: para penjahat kriminal semakin canggih, saat ini semakin sulit bagi korban yang tertipu untuk menentukan mana yang asli dan mana yang palsu.

Celah Untuk Serangan Siber.

Baru-baru ini telah dilakukan penelitian oleh organisasi kaspersky untuk mengetahui berapa banyak organisasi yang takut terhadap serangan siber yang berasal dari kesalahan personelnya. Lebih dari setengah organisasi yang disurvei percaya oleh karena sebab dari kurangnya pengetahuan, kecerobohan atau kedengkian di pihak personel dapat menyebabkan serangan siber. Penelitian tambahan menunjukkan 84% korban serangan siber disebabkan dari sebab tersebut diatas, ternyata sebagiannya adalah kesalahan manusia, menurut *KomputerWeekly.com (*Kaspersky, 2019). kesalahan personel seperti apa yang membuat organisasi Anda terbuka terhadap serangan siber. Berikut adalah

daftar tujuh kesalahan personel yang paling umum.

1. Membuka *Email* dari Orang Tak Dikenal. *Email* adalah bentuk komunikasi bisnis yang disukai. Rata-rata orang menerima 235 *Email* setiap hari, menurut Radicati Group. Dengan banyak *Email* itu, masuk akal bahwa beberapa adalah penipuan. Membuka *Email* yang tidak diketahui, atau lampiran di dalam *Email*, dapat melepaskan virus yang memberikan hacker *backdoor* ke ruang digital organisasi Anda.
2. Memiliki *Kredensial* Login yang Lemah. *Mashable* melaporkan bahwa 81% orang dewasa menggunakan kata sandi yang sama untuk semuanya. Kata sandi berulang yang menggunakan informasi pribadi, seperti nama panggilan atau alamat jalan, hal itu menjadikan masalah. *Sibercriminals* memiliki program yang menambang profil publik untuk kombinasi kata sandi potensial dan pasangan yang bisa sampai kemungkinan cocok sampai satu hits. Mereka juga menggunakan serangan kamus yang secara otomatis mencoba kata-kata yang berbeda sampai mereka menemukan kecocokan.
3. Meninggalkan Kata Sandi di kertas Catatan Tempel. Pernahkah Anda berjalan melalui kantor dan melihat kertas Catatan Tempel di layar dengan kata sandi tertulis di atasnya, hal Itu terjadi lebih sering daripada yang Anda pikirkan. Membiarkan kata sandi terlihat itu terlalu beresiko.
4. Memiliki akses ke segala sesuatu. Dalam beberapa kasus, organisasi tidak mengatur data. Dengan kata lain, semua orang dapat mengakses file organisasi yang sama. Memberi setiap orang akses yang sama ke data meningkatkan jumlah orang yang dapat membocorkan, kehilangan atau salah menangani informasi.
5. Kurangnya pelatihan personel yang efektif. Penelitian menunjukkan mayoritas organisasi memang menawarkan pelatihan *sibersecurity*. Namun, hanya 25% percaya hasil pelatihan iniefektif.
6. Tidak memperbarui perangkat lunak antivirus. Organisasi Anda harus menggunakan perangkat lunak antivirus sebagai tindakan perlindungan, tetapi seharusnya

tidak terserah kepada personel untuk memperbaruinya. Di beberapa organisasi, personel diminta untuk melakukan pembaruan dan dapat memutuskan apakah pembaruan berlangsung atau tidak. Personel mungkin mengatakan tidak untuk memperbarui ketika mereka berada di tengah-tengah proyek, karena banyak pembaruan memaksa mereka untuk menutup program atau me-*restart* komputer. Pembaruan antivirus penting, harus ditangani segera dan tidak boleh diserahkan kepada personel.

7. Menggunakan perangkat *mobile* tanpa jaminan. Banyak personel Anda memiliki ponsel, *tablet* atau *laptop*? Jika demikian, apakah Anda memiliki protokol untuk menjaga perangkat ini tetap aman? Banyak organisasi memiliki sikap longgar terhadap perangkat *mobile*, tetapi hal tersebut tetap menyajikan target yang mudah untuk *cybercriminals*.

Personel adalah manusia, dan kecelakaan digital bisa terjadi. Namun jika Anda mengambil langkah-langkah tertentu untuk melindungi perangkat dan melatih personel, Anda dapat mencegah ancaman siber. Tentu saja, mengelola keamanan siber organisasi Anda melampaui pendidikan personel. Melindungi jejak digital organisasi dan mengelola ancaman membutuhkan bantuan dari organisasi keamanan siber yang profesional.

Kesimpulan Rekomendasi dan Pembatasan.

Keamanan siber telah menjadi isu prioritas seluruh negara di dunia semenjak teknologi informasi dan komunikasi dimanfaatkan dalam berbagai aspek kehidupan terutama pada, pemerintahan, keamanan, pertahanan. Berbanding lurus dengan tingginya tingkat pemanfaatan teknologi informasi dan komunikasi tersebut, tingkat risiko dan ancaman penyalahgunaan teknologi informasi dan komunikasi juga semakin tinggi dan semakin kompleks.

Untuk menyikapi fenomena tersebut, TNI AL sebagai komponen utama dalam strategi pertahan laut pun, harus mampu untuk membangun kewaspadaan siber dengan menciptakan lingkungan siber yang strategis dan penyelenggaraan sistem elektronik yang aman, andal dan terpercaya. Dan juga membangun kesadaran dan kepekaan terhadap ketahanan dan keamanan

dalam ruang siber kepada personel TNI AL, agar dapat meminimalisir human error sebagai penyebab kebocoran data dan informasi. Melalui pembuatan aturan atau regulasi dengan sangsi yang terukur, kemudian menyusun sistem manajemen keamanan siber baik dalam bentuk software dan hardware untuk melindungi infrastruktur data kritis. Dalam rangka mewujudkan tujuan strategi pertahanan laut.

Daftar Pustaka.

BSSN. (2019). Laporan Tahunan 2019 Pusopskamsinas, BSSN. https://cloud. bssn.go.id/s/nM3mDzCkgycRx4S#pdfviewer

Kaspersky. (2019). *Cyber Security Awareness: 7 Ways Your Employees Make Your Business Vulnerable to Cyber Attacks*. https://www.kaspersky.com/resource-center/preemptive-safety/7-ways-to-cyberattack-vulnerability.

Holmes, D. (2005). *Communication theory: Media, technology, and society*. Sage.

Kuehl, D., & Pudas, T. (2010). Perspectives on building a cyber force structure. In *Proc. Conf. on Cyber Conflict* (pp. 163-181).

McDonnell, M. D., & Sayers, T. L. (2002). Information Systems Survivability in Nontraditional Warfare Operations. *Nontraditional Warfare: Twenty-First Century Threats and Responses*.

Gibson, W. (2019). Necromancer (1984). In *Crime and Media* (pp. 86-94). Rutledge.

Presiden RI. (2002). Undang-Undang RI Nomor 3 Tahun tentang Pertahanan Negara.

Presiden RI. (2017). Perpres No. 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN).

Menhan RI. (2014). Permenhan No. 82 Tahun 2014 tentang Pedoman Pertahanan Siber.

Komisi Eropa dan Direktorat Jenderal Untuk Penelitian dan Inovasi. (2020). Cybersecurity Jangkar Digital Kami Perspektif Eropa (pp. 15).