Jurnal TNI Angkatan Udara (Vol. 2 No.2, 2023)
ISSN: 2809-5464

SISTEM PENGAMANAN JARINGAN TERHADAP SERANGAN CYBER WARFARE

Rudy Damanik, Pratama Andika, Rahmayanti.
Rudidamanik02@gmail.com

ABSTRAKS — Memasuki pertumbuhan kemajuan industry 4.0 sebagai *fase* revolusi teknologi, sistem pengamanan jaringan menjadi suatu hal yang menjadi kebutuhan. Pengamanan jaringan sangat penting dan memegang peranan penting dari setiap aspek suatu organisasi. Oleh karenanya keamanan jaringan menjadi skala prioritas dalam pembangunan sistem yang ada saat ini. Dalam pembinaan dan penyelenggaraan sistem pengamanan yang ada di TNI AU sudah seharusnya menjadi sebuah organisasi yang bukan hanya untuk memudahkan pelaksanaan tugas satuan kerja saja, namun harus menjadi organisasi yang berkemampuan menjamin keamanan data serta sistem informasi yang dibangun. Mengoptimalkan pengamanan data sistem informasi memang bukanlah suatu hal yang mudah. Membutuhkan suatu perencanaan, pedoman, pelatihan serta keseriusan dari setiap unsur yang ada baik personel pelaksana di lapangan hingga pada level pimpinan. Untuk mencapai sasaran dalam pengoptimalan pengamanan data sistem dalam rangka mendukung tugas TNI AU, maka dibutuhkan langkah-langkah untuk meningkatkan kemampuan personel yang mengawaki organisasi dengan didukung peralatan infrastruktur yang dipadu dengan *prosedure* pengamanan yang ada menjadi faktor penting yang mutlak diperhitungkan serta direncanakan sehingga keamanan data lebih terjamin. Mewujudkan keamanan data sistem informasi pada hakekatnya merupakan serangkaian tahapan yang harus ditempuh dengan dukungan dari para pemangku kebijakan untuk merumuskannya. Hal ini dapat dimulai dari peningkatan kemampuan personel, revitalisasi infrastruktur data sistem informasi serta pembuatan prosedur keamanan data hingga organisasi baru yang khusus menangani kejahatan *cyber* hingga penguatan kepemilikan jaringan mandiri untuk mengintegrasikan seluruh sistem yang ada.

Kata Kunci : *Fase*, Revolusi, Teknologi pengamanan.

1. PENDAHULUAN

Komunikasi Data merupakan bagian dari teknologi komunikasi yang secara khusus berkenaan dengan transmisi atau peminda han data dan informasi di antara komputer dan piranti-piranti yang lain dalam bentuk digital yang dikirimkan melalui media komunikasi data. Informasi merupakan data yang telah disusun sedemikian rupa sehingga bermakna dan bermanfaat karena dapat dikomunikasikan kepada seseorang yang akan menggunakannya untuk membuat keputusan. Komunikasi data dan informasi merupakan bagian penting dari suatu sistem informasi karena merupakan pendukung penyediaan infra struktur yang memungkinkan perang kat keras yaitu komputer-komputer dapat berkomunikasi satu sama lain. Demikian juga komunikasi data dan informasi di TNI AU sangat erat kaitannya dengan infrastruktur pendukung dan sistem keamanan jaringan yang berpotensi terhadap bentuk serangan baik internal maupun eksternal TNI AU. Hal ini sesuai dengan tugas dari Satuan siber TNI AU yaitu melaksanakan penangkalan untuk melindungi infrastruktur informasi kritis TNI, yang meliputi aplikasi, sistem komputer dan jaringan dari berbagai macam dimensi ancaman ataupun serangan siber. Pengelolaan siber di TNI Angkatan Udara saat ini dihadapkan pada beberapa permasalahan, yang pertama pengelolaan jaringan masih dilaksanakan oleh masing-masing satuan kerja, hal ini terjadi karena belum terinteroprabilitinya setiap satuan dengan unit siber TNI Angkatan Udara, kedua sistem jaringan masih rentan terhadap kerusakan sistem jaringan yang disebabkan oleh virus,ketiga sistem jaringan rentan terhadap ancaman siber hal ini disebabkan oleh sistem pertahanan jaringan masih lemah, dan yang rentan terhadap pencurian

data/informasi hal ini disebabkan karena interkoneksi.

Mencermati kondisi dan permasalahan tentang sistem pengamanan jaringan satuan siber saat ini, maka diperlukan upaya yang harus dapat segera diterapkan untuk menindaklanjuti belum terinterope rabilitinya satuan kerja dengan unit siber TNI Angkatan Udara adalah dengan koordinasi, instalasi, konfigurasi jaringan, uji fungsi, kemudian upaya yang di laksanakan untuk mengantisipasi sistem jaringan yang masih rentan terhadap kerusakan adalah dengan pengadaan anti virus untuk server dan client, upaya yang dilakukan terhadap sistem jaringan yang rentan oleh ancaman siber adalah instalasi dengan menjalankan beberapa prosedur pencegahan, penangkalan, dan pemuli han, sedangkan upaya yang dilaksana kan terhadap kerentanan pencurian data/ informasi akibat inter koneksi adalah dengan enkripsi data dan pembuatan *open* VPN di jaringan internet.

2. LANDASAN

Pancasila sebagai Landasan Idiil. Pancasila merupakan ideologi dan pandangan hidup bangsa Indonesia dimana didalamnya mencerminkan cita-cita besar segenap bangsa Indonesia dalam menjalani kehidupan bermasya rakat semakin beradap semakin ber bhineka tunggal ika.

UUD 1945 Sebagai Landasan Konstitusional. Pada Pembukaan UUD 1945 alinea ke 4 dengan tegas dan jelas di amanatkan tentang implementasi pelaksanaan tugas TNI sebagai alat pertahanan negara. Hal ini dijabarkan lebih lanjut terdapat pada batang tubuh UUD 1945 Bab XII tentang Pertahanan Negara pasal 30 ayat 3 menyatakan bahwa Tentara Nasional Indonesia terdiri atas Angkatan Darat, Angkatan Laut, dan Angkatan Udara sebagai alat negara bertugas mempertahankan, melindungi dan memelihara keutuhan dan kedaulatan negara.

Wawasan Nusantara Sebagai Landasan Visional. Landasan visional atau tujuan nasional wawasan nusantara sebagai wawasan nasional bangsa indonesia merupakan ajaran yang diyakini kebe narannya oleh seluruh rakyat dengan tujuan agar tidak terjadi penyesalan dan penyimpangan dalam rangka mencapai dan mewujudkan cita-cita dan dan tujuan nasional yang tercantum dalam pembukaan UUD 1945.

Ketahanan Nasional Sebagai Landasan Konsepsional.
Ketahanan nasional adalah suatu kondisi bangsa yang dinamik meliputi aspek kehidupan nasional yang terintegrasi berisi ketangguhan dan keuletan yang mengan dung kemampuan mengembangkan ke kuatan nasional dalam menghadapi dan mengatasi segala ancaman, gangguan, hambatan dan tantangan.

Undang-Undang RI Nomor 3 Tahun 2002 Tentang Pertahanan Negara.
Sistem pertahanan negara adalah sistem pertahanan yang bersifat semesta yang melibatkan seluruh warga negara, wilayah dan sumberdaya nasional lainnya, serta disiapkan secara dini oleh Pemerintah dan diselenggarakan secara total, terpadu, terarah dan berlanjut untuk menegakkan kedaulatan negara, keutuhan wilayah dan keselamatan bangsa dari segala macam jenis ancaman dan gangguan.

Undang Undang RI Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia.
Salah satu tugas pokok lainnya TNI adalah memberdayakan wilayah pertahanan dan kekuatan pendukungnya secara dinisesuai dengan sistem pertahanan semesta, dimana penggunaan satuan siber sebagai kekuatan pertahanan baru dalam menghadapi adanya ancaman siberyang semakin berkembang. Ancamanterhadap serangan tersebut tidak boleh dianggap remeh dan harus menjadi agenda baru TNI nantinya dalam penyusunan doktrin pertahanan yang baru dengan mempertimbangkan kekuatan siber sebagai kemampuan untuk bertahan dan keutuhan NKRI sehingga dapat dijadikan

TNI dalam langkah-langkah penangkalan dan penindakan terhadap bahaya serangan siber.

Peraturan Menteri Pertahanan RI Nomor 38 Tahun 2011 tentang Kebijakan Sistem Informasi Pertahanan Negara. Peraturan ini menyampaikan bahwa pembangunan teknologi informasi dan komunikasi bidang pertahanan diarahkan untuk meningkatkan kualitas sistem informasi pertahanan negara termasuk pertahanan siber, yang didalam nya dilakukan secara bertahap, berkesi nambungan dan terintegrasi dalam penge lolaan pertahanan negara.

Peraturan Menteri Pertahanan RI Nomor 68 Tahun 2014 Tentang Pengamanan Informasi di Lingkungan Kementerian Pertahanan dan TNI.
TNI AU merupakan salah satu instansi pemerintah di bidang pertahanan matra udara yang memiliki kepentingan untuk mengamankan semua sistem elektronik dan jaringan informasi di lingkungannya sesuai dengan doktrin yang dimiliki. Urgensi pembentukan jaringan satuan pertahanan siber TNI AU ditujukan untuk mengantisipasi datangnya ancaman dan serangan siber yang terjadi dan juga untuk berkoordinasi dengan pengamanan siber di sektor-sektor lainnya sesuai kebutuhan.

Peraturan Menteri Pertahanan RI Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber.
Pertahanan siber adalah suatu upaya untuk menanggulangi serangan siber yang menyebabkan terjadinya ganggunan terhadap penyelenggaraan peratahanan negara. TNI AU merupakan salah satu instansi pemerintah di bidang pertahanan matra udara yang memiliki kepentingan untuk mengamankan semua sistem elektronik dan jaringan informasi di lingkungannya sesuai dengan doktrin yang dimiliki.

Peraturan Panglima TNI Nomor 17 Tahun 2017 tantang Organisasi dan Tugas Siber TNI.

Teknologi informasi yang berkembang sangat pesat dapat memberikan manfaat dan kemudahan kepada organisasi sekaligus menimbulkan kerawanan dan ancaman. Pembentukan sistem informasi internal TNI AU secara terpadu dan bersinergi sangat dibutuhkan sebagai implementasi sistem pengama nan jaringan satuan siber guna meng hadapi ancaman siber sebagai salah satu bentuk perwujudan upaya perlindungan dan pengamanan data dan informasi TNI AU dalam mendukung tugas TNI AU, yang merupakan bagian dari TNI sebagai alat pertahanan negara matra udara.

Keputusan Kasau Nomor Kep/571/X/2012 tanggal 24 Oktober 2012 tentang Doktrin TNI AU Swa Bhuwana Paksa. Dalam Doktrin TNI AU Swa Bhuwana paksa Pada Bab IV pasal 18 ayat d. dijelaskan bahwa penggunaan kekuatan udara dalam upaya pertahanan Negara dilakukan melalui beberapa bentuk operasi udara, baik yang bersifat matra tunggal maupun sebagai bagian dari suatu operasi gabungan. Dimana salah satu kemampuan dan kekuatan udara adalah kemampuan eksploitasi Informasi. Dengan adanya kemampuan eksploitasi informasi maka pemanfaatan dan pendaya gunaan informasi dimaksudkan untuk mendapatkan, memanfaatkan dan men dayagunaan informasi melalui ruang (wahana) dirgantara dalam rangka menda patan keunggulan informasi agar tercipta penguasaan udara. Dalam rangka me wujudkan hal tersebut maka implementasi sistem pengamanan jaringan satuan siber guna menghadapi ancaman siber sangat dibutuhkan dalam mendukung tugas TNI AU, yang merupakan bagian dari TNI sebagai alat pertahanan negara matra udara.

3. METODOLOGI

Teori Keunggulan Informasi Dalam Perang. Informasi memainkan peran yang sangat penting dalam kemenangan perang baik itu konvensional maupun non konven sional. Pihak yang bertikai

berusaha untuk memperoleh informasi secepat dan seakurat mungkin tentang

situasi musuh dan daerah operasi untuk menentukan strategi yang efektif. Dalam teori Perang Tsun Zu mengemukakan bahwa “siapa yang berhasil mengetahui tentang kemampuan musuh, kemampuan diri sendiri serta keadaan lingkungan secara baik, dia akan memenangkan peperangan”. Teori tersebut tetap relevan sesuai dengan perkembangan zaman, bahkan kemudian muncul istilah pe perangan informasi yaitu usaha untuk menggagalkan sistem informasi musuh dan berusaha melindungi sistem informasi sendiri.

Teori Peperangan (C*yber Warfare*). Czosseck dan Geers (2009) menyatakan perlunya para ahli strategi kontemporer untuk memahami, bahwa dewasa ini terdapat kecenderungan dimana ada bagian dari setiap konflik di dunia nyata yang akan mengambil tempat di dunia maya (*virtual*). Informasi adalah sasaran utama dari operasi Informasi karena siapapun yang menguasai informasi maka akan memenangkan peperangan. Salah satu cara untuk menguasai informasi adalah dengan menguasai media pengo lahan, penyimpanan dan pertukaran informasi yakni sistem komputer, jaringan komputer, jaringan telekomunikasi, dan peralatan berbasis prosesor serta pengen dali *embedded* dan Internet melalui *cyber space* dengan menggelar *cyber operations*.

Teori Siber Dalam Perang Informasi. *Cyber Space* (dunia maya) adalah suatu mandala perang yang setara dan mirip dengan daratan, udara, laut dan ruang angkasa. Seperti halnya penguasaan keunggulan laut, baik dipermukaan maupun operasi dibawah air maka penguasaan ruang udara juga dapat dilakukan melalui operasi udara, sama halnya dengan keunggulan pada dunia maya dapat dilaksanakan dengan menguasai sistem jaringan elektronik dan dengan penguasaan secara penuh dari spektrum frekuensi.Penggunaan kekuatan siber dapat dilakukan oleh siapa saja dengan biaya yang tidak terlalu mahal (jika dibandingkan dengan senjata dan pesawat tempur) tapi dapat meng

akibatkan kerusakan yang fatal seperti lumpuhnya sistem radar, komunikasi, penerbangan dan kodal musuh.

PERMASALAHAN

Berkembangnya teknologi informasi khususnya jaringan komputer dan layanan-layanannya di satu sisi dapat mempermudah pekerjaan-pekerjaan yang begitu kompleks, akan tetapi di sisi lain timbul masalah yang sangat serius, yakni faktor keamanannya. Untuk mencegah terjadinya kejahatan siber, seperti menye rang suatu jaringan komputer, menyusup kedalam suatu jaringan untuk mengambil data yang bersifat rahasia dan melum puhkan suatu sistem jaringan, maka perlu diambil suatu langkah dalam pengamanan pada suatu sistem jaringan komputer agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan dengan membuat suatu sistem keamanan yang dapat menangkal serangan dan usaha penyusupan baik dari sisi external dan internal suatu sistem jaringan komputer. Oleh karena itu sistem pengamanan jaringan yang standar harus mencakup beberapa prinsip yaitu keamanan berlapis, akses kontrol, keamanan peran tertentu, kesadaran pengguna, monitoring, men jaga sistem terus diperbaharui dan adanya tim respon.

Satuan Siber Belum Berfungsi Sebagai Puskodal Sistem Pengamanan Jaringan Komunikasi Data TNI AU. Saat ini Satuan Siber belum dapat melaksanakan sistem monitoring atau puskodal. Monitoring merupakan salah satu aspek keamanan yang berfungsi untuk memonitor sistem dan memastikan bahwa jaringan komputer yang tergelar aman target serangan siber. Hal ini menunjukkan bahwa satuan siber harus berfungsi sebagai pusat komando dan kendali dari semua sistem jaringan yang tergelar. Namun, saat ini Satuan siber belum berfungsi sebagai Puskodal,

dikarena kan masing-masing satuanmasih menggelar jaringan secara mandiri. Satuan ini menggelar jaringannya untukmemanfaatkan teknologi informasisebagai alat bantuyangdapat me

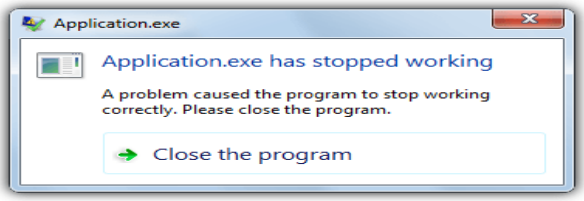
mudahkan dan mem percepat tugas-tugas yang dihadapi. Adapun manfaat dari sistem jaringan komputer adalah sebagai berikut:

- *Sharing resources* bertujuan agar seluruh program, peralatan atau peri pheral lainnya dapat dimanfaatkan oleh setiap orang yang ada pada jaringan komputer tanpa terpengaruh oleh lokasi maupun pengaruh dari pemakai.
- Media komunikasi memungkinkan terjadinya komunikasi antar pengguna, baik untuk telecon ference maupun untuk mengirim pesan atau informasi yang penting lainnya.
- Integrasi data dapat mencegah keter gantungan pada komputer pusat, karena setiap proses data tidak harus dilakukan pada satu komputer saja, melainkandapat didistribusikan ke tempat lainnya.
- Pengembangan dan pemeliharaan dapat dilakukan dengan mudah dan meng hemat biaya, karena setiap pembelian komponen seperti printer, maka tidak perlu membeli printer sejumlah komputer yang ada tetapi cukup satu buah karena printer itu dapat digunakan secara bersama-sama untuk memudahkan pemakai nya dalam merawat harddisk dan peralatan lainnya, misalnya untuk mem berikan perlindungan ter hadap serangan virus maka pemakai cukup memusatkan per hatian pada hardisk yang ada pada komputer pusat.
- Keamanan data dapat memberi kan perlindungan terhadap data. Karena pemberian dan pengaturan hak akses kepada para pemakai, serta teknik perlin dungan terhadap harddisk sehingga data mendapat kan perlindungan yang efektif.
- Sumber daya lebih efisien dan infor masi terkini pemakaian sumber daya secara bersama-sama, akan mendapat kan hasil yang maksimal dan kualitas yang tinggi. Selain itu data atau informasiyang diakses selalu terbaru, karena setiap ada perubahan yang terjadi dapat segera langsung diketahui oleh setiap pemakai.

Sistem Operasi Jaringan Rentan Kerusakan.

Sistem operasi jaringan (Inggris: *network operating system*) adalah sebuah jenis sistem operasi yang ditujukan untuk menangani jaringan. Sistem operasi jaringan yang ada pada saat ini selalu mengalami gangguan pada sistem jaringan yang mengakibatkan data dan sistem informasi yang tersedia tidak dapat diakses dikarenakan database error, OS jaringan dan server error, perubahan pada kode program aplikasi. Untuk lebih jelas dapat dilihat contoh program aplikasi yang error.

Gambar 3.1 Pesan Error pada Aplikasi



Sistem Jaringan Rentan Terhadap Ancaman Siber. Saat ini teknologi komputer merupakan salah satu teknologi yang mengalami perkembangan yang sangat cepat, sehingga keamanan akan data dan informasi sangat dibutuhkan, hal ini akan signifikan terhadap sistem pengamanan jaringan yang kurang kuat baik dari sisi perangkat keras maupun perangkat lunaknya. Adapun ancaman cyber atau serangan cyber menurut Cordesman dalam buku Syaiful Anwar yang berjudul "Melindungi Negara" menyatakan bahwa serangan cyber terdiri dari 5 (lima) jenis utama seranganyaitu:

- *A Cyberattack on the specific database of an owner/operator*, adalah serangan cyber ini ditujukan pada basis data spesifik dari operator. Serangan cyber yang dilakukan oleh para hacker dapat masuk ke basis data sehingga data-data dapat dikuasai sepenuhnya. Seperti, Basis data Google di daratan Tiongkok pernah menjadi sasaran kelompok hacker, di mana kelompok hacker membobol basis data Google di Tiongkok ini berniat mengakses dan berusaha juga mendapat informasi dari akun GMail aktivis hak asasi

manusia Negeri Tirai Bambu tersebut.

- *A Cyberattack for the purpose of gaining acces to network*, maksudnya adalah untuk tujuan mendapatkan akses ke jaringan. Jenis kejahatan ini terjadi ketika seseorang memasuki atau menyu sup ke dalam suatu sistem jaringan

komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Hal ini biasa dilakukan oleh hacker dan creacker untuk menyusup dan berusaha masuk untuk dapat akses ke jaringan. Hacker dan Cracker membuat komunitas dengan membuat server sendiri untuk mencuri sinyal secara paksa dan tanpa izin ke setiap provider penyedia layanan internet. Hacker dan Cracker dalam kasus ini menggunakan teknik SSH Tunneling, yaitu teknik yang dipakai sebagai back door dari dunia luar langsung menembus ke dalam “Behind Enemy Lines” melewati semua firewall, IDS, IPS, atau apapun itu di perbatasan protokol jaringan.

- *A Cyberattack for the purpose of espionage*, maksudnya adalah serangan siber untuk tujuan mata-mata. *Cyber Espionage* merupakan kejahatan yang memanfaatkan beberapa jaringan internet untuk mela kukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. *Sabotage and Extortion* merupakan jenis kejahatan yang di lakukan dengan mem buat gangguan, perusakan atau penghancuran ter hadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.
- *A Cyberattack for the purpose of shutting down service*, maksudnya adalah Serangan Cyber untuk tujuan mematikan layanan seperti serangan DDos yangmana akan mematikan server dan menyi bukkan server. Teknik ini disebut sebagai traffic flooding. Selain itu DDos juga mem banjiri jaringan dengan banyak request terhadap sebuah layanan jaringan yang disedakan oleh sebuah host sehingga request yang datang dari pengguna terdaftar tidak dapat dilayani oleh layanantersebut.
- *A Cyberattack for the harmful instruc tions*, adalah serangan Cyber untuk instruksi berbahaya, seperti Botnet yang merupakan kegiatan menyusupkan beberapa program ter tentu kepada server-server komputer dimana program-program tersebut biasanya disusupkan sebagai Worms, Trojan horse, atau Backdoors, di bawah perintah Master Refer dan dikendalikan dengan sebuah

remote, sehingga program tersebut dapat bekerja kapan saja sesuai keinginan si Master tadi yang tujuannya untuk mengganggu ataupun merusak suatu jaringan atau sistem operasi computer, saat ini Indonesia merupakan negara yang beresiko tinggi mengalami serangan Siber, hal ini dapat dilihat pada gambar berikut:

Gambar 3.2 Resiko Serangan IT Security di Indonesia

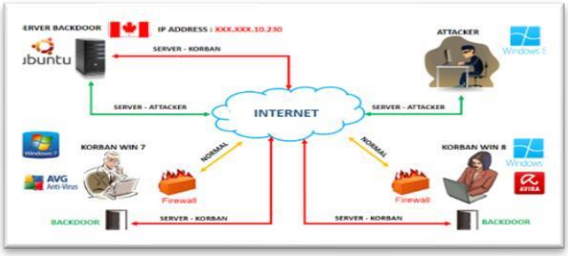
Sistem Jaringan Rentan Terhadap Pencurian Data, adalah data-data penting dan ada dua bentuk aktivitas ter hadap jaringan komputer, yaitu hacking dan cracking. Hacking adalah usaha memasuki sebuah jaringan dengan maksud mengeksplorasi atau mencari kelemahan sistem jaringan secara ilegal. Sedangkan cracking adalah usaha memasuki sebuah jaringan secara ilegal dengan maksud mencuri, mengubah,atau menghancurkan file atau data yang disimpan di komputer-komputer yang ada di jaringan tersebut. Dengan mengguna kan tool-tool tersebut, seorang hacker dan cracker dapat melihat langsung kemam puan pengamanan dan keamanan sebuah jaringan komputer. Kemudian mereka memanfaatkan kelemahan jaringan komputer tersebut untuk melaku kan penyusupan antara lain:

- *Spoofing,* cara menyusup dengan memalsukan identitas user sehingga hacker bisa login ke sebuah jaringan komputer secara ilegal.

- *Scanner*, secara otomatis akan mende teksi kelemahan sistem keamanan sebuah jaringan komputer di jaringan lokal ataupun komputer di jaringan lain.
- *Sniffer*, sebagai penganalisis jaringan dan bekerja untuk memonitor jaringan komputer.
- *Password Craker*, membuka pass word yang sudah dienkripsi.

- *Session Hijacking*, adalah suatu kegiatan yang berusaha untuk me masuki (menyusup) ke dalam sistem melalui sistem operasional lainnya yang di jalankan oleh seseorang (pelaku: Hacker). Session Hijacking merupakan aksi pengambilan kendali session milik user lain setelah sebelumnya "pembajak" berhasil memperoleh autentifikasi ID session yang biasanya tersimpan dalam cookies. Adapun bentuk pencurian data dapat dilihat lebih jelas pada gambar berikut ini:

Gambar 3.3 Pencurian data oleh hacker.



Sistem Pengamanan Jaringan Satuan Siber berimplikasi pada:

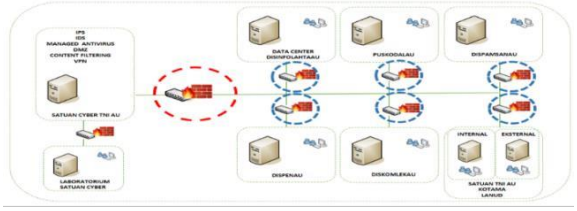
- Kondisi jaringan satuan siber TNI AU yang belum berfungsi sebagai Puskodal maka akan berdampak pada tidak ter integrasinya Satuan Siber dengan satuan-satuan TNI AU sehingga tidak dapat mengatasi ancaman Siber.
- Sistem operasi jaringan rentan terhadap kerusakan yang disebabkan oleh virus akan mengakibatkan data dan sistem informasi yang tersedia tidak dapat diakses.
- Sistem jaringan rentan terhadap ancaman siber yang disebabkan sistem jaringan yang lemah maka akan meng akibatkan rentan terhadap serangan siber.
- Sistem jaringan rentan terhadap pencurian data yang disebabkan oleh interkoneksi maka akan menyebabkan peluang bagi para hecker untuk mencuri data dan informasi.

Menghadapi Ancaman Siber berimplikasi pada:

- Tidak terintegrasinya Satuan Siber dengan satuan-satuan TNI AU maka tidak dapat mengatasi ancaman Siber sehingga tidak dapat mengamankan komunikasi data dan informasi TNI AU.
- Kerusakan yang disebabkan oleh virus akan mengakibatkan data dan sistem informasi yang tersedia tidak dapat diakses sehingga tidak dapat meng amankan komunikasi data dan informasi TNI AU.
- Sistem jaringan yang lemah maka akan mengakibatkan rentan terhadap serangan siber sehingga tidak dapat mengamankan komunikasi data dan informasi TNI AU.
- Interkoneksi menyebabkan peluang bagi para hecker untuk mencuri data dan informasi sehingga data dan informasi TNI AU tidak aman.

Sistem Jaringan Satuan Belum Terintegrasi Dengan Satuan Siber, merupakan penyatuan unsur-unsur dari sesuatu yang berbeda atau beraneka ragam sehingga menjadi satu kesatuan dan pengendalian terhadap konflik atau penyimpangan dari penyatuan unsur-unsur data yang merupakan suatu proses menggabungkan atau menyatukan data yang berasal dari sumber yang berbeda dalam rangka mendukung manajemen informasi dan mendukung pengguna untuk melihat kesatuan data. Sedangkan, konfigurasi integrasi sistem operasi jaringan adalah konfigurasi yang dilakukan agar antar sub sistem saling keterkaitan sehingga data dari satu sistem secara rutin dapat melintas, menuju atau diambil oleh satu atau lebih sistem yang lain. Kondisi saat ini satuan cyber belum dapat melakukan interopability dikarenakan jaringan komputer tiap-tiap satuan dengan satuan cyber belum terkonfigurasi. Berikut adalah gambar yang menunjukan bahwa sistem jaringan tiap satuan dan satuan cyber belum terintegrasi.

Gambar 3.4 Jaringan Belum Terintegrasi



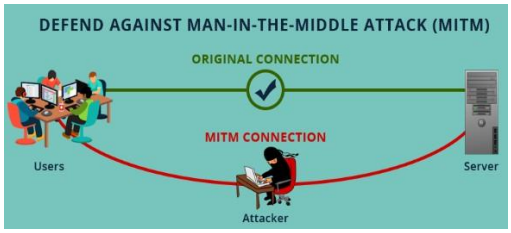
Gambar lingkaran merah adalah router management yang dapat memadukan seluruh sistem jaringan. Router manage ment ini terdiri dari:

- *Router Statis/Static Router*. Dalam penggunaan static router bahwa proses penghalaan pada router ini diadministra sikan secara manual oleh seorang administrator. Namun pada saat ini, Router Statis yang tergelar pada tiap-tiap satuan belum dikonfi gurasi sehingga tidak dapat terkoneksi dengan router statis yang ada di satuan siber.
- *Router dinamis/Dynamic Router.* proses routing murni diatur oleh seorang administrator jaringan, maka padadynamic router, proses routing akan berjalan secara otomatis dan juga dinamis.Semua proses itu dilakukan secara dinamis oleh router secara otomatis.
- *Wireless Router*, jenis router statis maupun router dinamis. Wireless Router yang tergelar pada tiap-tiap satuan belum dikonfigurasikan sehingga wireless router yang ada di setiap satuan belumterkoneksi dengan router statis yang ada di satuan dimana router satuan ini harus terkoneksi dengan satuan siber.

Adanya ancaman virus. Virus komputer merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. Virus yang biasa menyerang adalah virus Trojanhorse atau Kuda Troya atau yang lebih dikenal sebagai Trojan dalam keamanan komputer merujuk kepada sebuah bentuk perangkat lunak yang mencurigakan (*malicious software/ malware)* yang dapat merusak sebuah sistem atau jaringan. Tujuan dari Trojan adalah memperoleh informasi dari target (password, kebiasaan user yang tercatat dalam system log, data, dan lain-lain), dan mengendalikan target (memperoleh hak akses pada target).

Sistem keamanan jaringan yang masih lemah. Keamanan jaringan komputeradalah proses untuk mencegah dan mengiden tifikasi penggunaan yang tidak sah dari jaringan komputer. Tujuan Keamanan jaringan komputer adalah untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logik baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer. Seperti gambar berikut ini:

Gambar 3.5 Sistem pengamanan jaringan

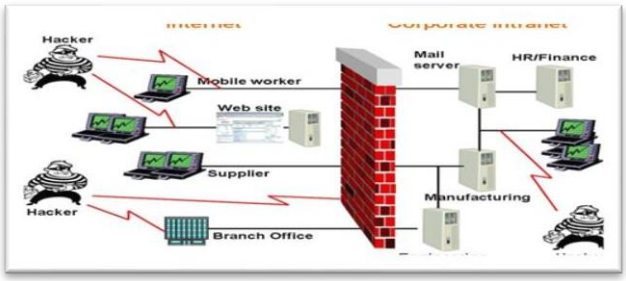


Hal ini disebabkan karena sistem hardening hostnya lemah. Adapun elemen-elemen dari hardening host adalah:

- Kriptografi, adalah suatu ilmu yang mempelajari bagaimana cara agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga.
- *Firewall,* merupakan *hardware, software* maupun sistem itu sendiri yang tujuannya melindungi komputer dalam jaringan, baik melakukan filterasi, membatasi ataupun menolak permintaan koneksi layanan luar jaringan.
- *Intrusion Detection System* (IDS), merupakan cara melakukan otomati sasi pengawasan pada penyusup. IDS mendeteksi jenis serangan pada aktifitas jaringan.

Interkoneksi, yaitu keterhubungan antar-jaringan telekomunikasi dari penye lenggara jaringan telekomunikasi yang berbeda. Interkoneksi antar-operator telekomunikasi wajib dilaksanakan di Indonesia untuk memberikan jaminan kepada pengguna agar dapat mengakses jasa telekomunikasi keterhubungan ini

dapat dimanfaatkan hacker untuk melaku kan pencurian dan pemanfaaatan data-data sebagai orang yang tidak berhak. Halini disebabkan karena Seperti terlihat pada gambar dibawah ini:



Gambar 3.6 Hacker memanfaatkaninterconection

Pengaruh Lingkungan Global
Perkembangan lingkungan strategis dunia saat ini merupakan produk globalisasi yang didorong oleh perkembangan iptek yang meliputi teknologi informasi dan komunikasi, *cyber,* bioteknologi, pesawat terbang tanpa awak (PTTA), teknologi robotik dan teknologi persenjataan khusus nya senjata pemusnah massal ber kembang sangat pesat. Globalisasi dengan segala pengaruhnya telah mem bawa pertahanan negara-negara dunia menjadi tergantung pada perang dengan teknologi informasi dan komunikasi.

Pengaruh Lingkungan Regional
Perkembangan situasi menonjol di kawasan Asia Tenggara yang ber pengaruh terhadap kepentingan nasional Indonesia adalah sengketa perbatasan. Kawasan Asia Tenggara masih diwarnai dengan permasalahan sengketa per batasan yang sampai dengan saat ini belum mencapai penyelesaian.

Pengaruh Lingkungan Nasional. Perkembangan lingkungan strategis dalam negeri dipengaruhi beberapa aspek gatra yaitu meliputi:

Geografi. Letak geografi Indonesia sangat strategis, yaitu diantara benua Asia dan Australia serta diantara samudera Pasifik dan samudera India sehingga sering digunakan sebagai jalur lalu lintas inter nasional. Indonesia juga terletak pada lingkaran cincin api (*ring of fire*) yang memiliki potensi ancaman tinggi terhadap bencana alam karena berada diantara wilayah lintasan dua jalur pegunungan yaitu pegunungan Sirkum Pasifik dan Sirkum Mediterania.

Demografi. Indonesia merupakan negara dengan penduduk terbanyak ke-4 di dunia. Jumlah penduduk yang banyak dan tidak diimbangi dengan tersedianya lapangan pekerjaan serta peningkatan kualitas SDM merupakan potensi kerawanan dalam bentuk penggalangan dari kelompok- kelompok radikal dan pihak asing serta munculnya konflik yang dapat merugikan Indonesia. Guna mencegah dan meng antispasi ancaman siber tersebut perlu dikembangkan sistem pengamanan jaringan satuan siber TNI AU dalam pengamanan komunikasi data dan informasi.

Ideologi. Implementasi pengamalan ideologi Pancasila dalam kehidupan ber bangsa dan bernegara mengalami degradasi. Masih terdapat keinginan dari sebagian masyarakat Indonesia untuk merubah ideologi Pancasila dengan syariat Islam serta ajaran sosialis dan komunis, sehingga dapat membahayakan keutuhan bangsa dan negara.

Politik. Perkembangan situasi politik akan lahir kebijakan nasional yang mencakup berbagai aspek kehidupan bermasyarakat, berbangsa, dan bernegara. Salah satunya dengan memanfaatkan teknologi informasi khusunya internet dirasa sangat efektif dalam menyebarluaskan pengaruh dan provokasinya karena media internet merupakan media yang tanpa batas baik waktu maupun temat.

Ekonomi. Tingkat inflasi yang semakin menekan nilai rupiah merupakan hal yang harus diantisipasi agar penurunan nilai tukar rupiah tidak terus berlanjut sehingga mengganggu stabilitas ekonomi nasional. Kondisi ini dapat menyebabkan anggaran pertahanan belum menjadi prioritas sehingga mempengaruhi dukungan

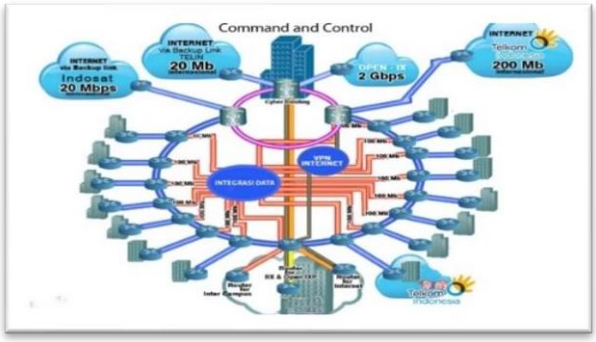
anggaran untuk mengembangkan sistem pengamanan jaringan satuan siber yang dialokasikan pada TNI AU.

Sosial Budaya. Pesatnya perkembanganteknologi informasi yang memanfaatkan teknologi satelit, UAV dan jaringan internettelah memberikan kemudahan dalam pengumpulan informasi. Bentuk ancaman*cyber* dapat digolongkan menjadi beberapa jenis, antara lain *unauthorized access*, *illegal contents*, penyebaran virus secara sengaja, *data forgery*, *cyber espionage*, *sabotage and extortion*, *cyberstalking*, *carding*, *hacking and cracker*, *cybersquatting and typosquatting*, *hijacking*, serta *cyber terrorism*.

Pertahanan dan Keamanan, Salah satu upaya yang dapat dilakukan untuk

membangun rasa kebersamaan dan mengurangi ancaman disintegrasi bangsa ialah dengan menerapkan Sistem Pertahanan Keamanan Rakyat Semesta (Sishankamrata), yang digunakan sebagai pendukung dalam penggunaan teknologi informasi oleh TNI AU perlu dilaksanakan sebagai bagian dari alat pertahanan negara dalam rangka pengembangan sistem penga manan jaringan satuansiber.

Sistem Pengamanan Jaringan Satuan Siber Berfungsi Sebagai Puskodal Sistem Pengamanan Jaringan Komunikasi Data TNI AU. Seluruh jaringan yang ada disatuan sudah dipadukan dan dikonfigurasikan sehingga menjadi satu sistem jaringan yang utuh dan sudah dapat di kontrol oleh satuan cyber. Berikut adalah gambar yang menunjukan bahwa sistem jaringan tiap satuan dan satuan cyber sudah Terintegrasi.

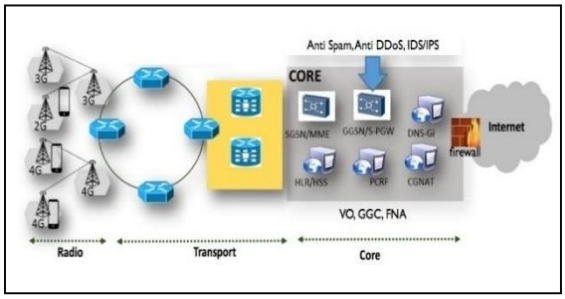


Adapun perangkat-perangkat jaringan komputer yang digunakan seperti router statis, router dinamis, wireless routersudah dikonfi gurasi dimana pengamatan atau pengklasifikasian IP Address sudah diatur dan di manajemen sehingga komunikasi data dapat berjalan dengan baik tanpa adanya konflik pada sistem jaringan.

Sistem operasi jaringan andal, untuk melayani pengguna, seperti layanan berbagi berkas, layanan berbagi alat pencetak (printer), DNS Service, HTTP Service, dan lain sebagainya yang ada pada saat ini tidak lagi mengalami gangguan pada sistem jaringan sehingga data dan sistem informasi yang tersedia aman dan dapat diakses, tidak terjadi kerusakan pada database, OS jaringan

dan server serta tidak terjadi lagi perubahan pada kode program aplikasi.

Gambar 5.1 Sistem Operasi Jaringan yang Terlindungi

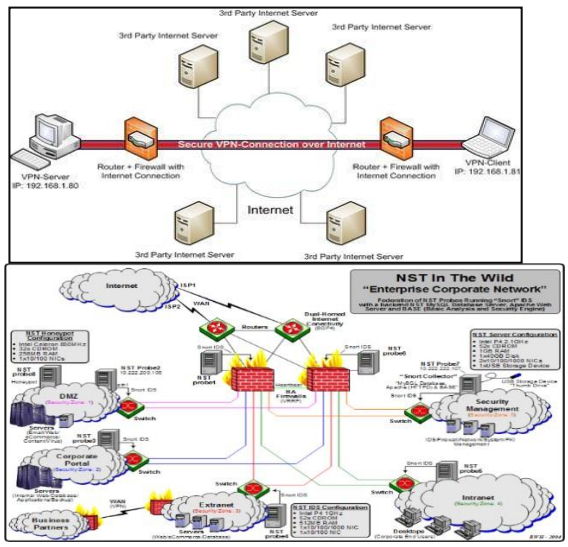


Pada gambar 5.1 menunjukan bahwa di dalam jaringan internet yang berbasis kabel, telah dipersiapkan fungsikeamanan seperti Antispam, Anti DDoS, Firewall, IDS dan IPS yang membentengi serangan virus atau malware serta penggunaan perangkat IDS/IPS yang mencegah masuknya paket berbahaya dengan memasukkan program jahat melalui cookies, email dengan attach ment, atau unduh file dan aplikasi yang telah disisipi

program jahat.

Sistem Keamanan Jaringan Anda Terhadap Ancaman Siber, diharapkan aman dari serangan siber yang menyerang basis data spesifik dari operator, serangan terhadap penyusupan ke dalam suatu sistem jaringan komputersecara tidak sah atau tanpa izin, serangan espionase, dan serangan denganpenyusupan program-program tertentu kepada server-server komputer dimana program-program yang Worms, Trojan horse, atau Backdoors.

Gambar 5.2 Sistem Operasi Jaringan yangTerlindungi

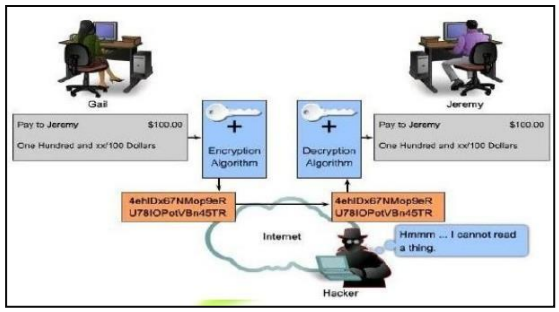


Gambar 5.2 Menunjukkan bahwa sistem operasi jaringan sudah bekerja dimana fungsi firewall, fungsi security jaringan dan pengamanan terhadap perangkat router dapat menghalangi masuknya

serangan siber dalam sistem jaringan yang sudah digelar baik di jaringan satuan terkecil sampai jaringan satuan yang terbesar.

Sistem jaringan andal terhadap pencurian data dan informasi. Keandalan sistem jaringan sudah terjamin keamanannya karena perangkat jaringan sudah terlindungi dari bentuk ancaman pencurian data yaitu dengan meng aktifkan firewall, kriptografi atau penyan dian yang kuat, pemasangan dengan Secure Socket Layer (SSL) untuk menyandikan data pada perangkat jaringan dan penggunaan open VPN.

Gambar 5.3 VPN Pada Jaringan Internet



Pada gambar 5.3 bahwa VPN melakukan interkoneksi jaringan dengan jalurtersendiri namun melalui jaringan wide dan juga mengisolir hubungan luar dengan berbagai encrypsi sehinggajaringan yang terbentuk seolah-olah terlihat sebagai local network.

Gambar 5.4 Proses Enkripsi pada Jaringan

Pada gambar 5.4 bahwa hacker berusaha untuk masuk kedalam jaringan dan bermaksud mencuri data namun kesulitan karena di jaringan sudah diamankan dengan enkripsi dimana adanya suatu proses pada informasi atau data yang hendak dikirim, diubah menjadi bentuk yang hampir tidak dapat dikenali sebagai

informasi pada awalnya dengan menggu nakan algoritma tertentu.

Sistem pengamanan jaringan satuan siber menghadapi ancaman siber dalam rangka mengamankan komunikasi data dan informasi TNI AU

- Satuan Siber TNI AU yang sudah berfungsi sebagai puskodal maka akan berdampak pada terintegrasinya satuan-satuan siber TNI AU dalam satu kesatuan komando sehingga memudahkan dalam mengatasi ancaman Siber.
- Sistem operasi jaringan yang andal terhadap serangan oleh virus akan menguatkan sistem operasi jaringan sehingga terhindar dari kerusakan serta penguatan sistem jaringan siber sehingga terhindar dari serangan siber.
- Pencurian data yang disebabkan oleh

interkoneksi tidak akan lagi memberi peluang bagi para hecker untuk mencuri data dan informasi.

- Terintegrasinya Satuan Siber dengan satuan-satuan TNI AU maka dapat meng atasi ancaman Siber sehingga dapat mengamankan komunikasi data daninformasi TNI AU serta kerusakan yang disebabkan oleh virus tidak lagi ditemukansehingga data dan informasi dapat diakses secara normal dan lancar kemudian keamanan komunikasi data dan informasiTNI AU dapat terlaksana dengan baik.
- Sistem jaringan yang sudah kuat dan tidak lagi rentan terhadap serangan siber maka keamanan komunikasi data dan informasi TNI AU dapat terwujudkan dan tidak lagi memberikan peluang bagi para hecker untuk melakukan pencurian data dan informasi sehingga data dan informasiTNI AU menjadi aman.

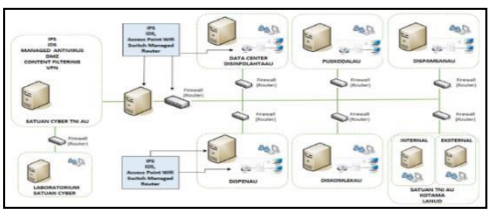
4. STRATEGI KEBERHASILAN

Strategi Sistem Jaringan Satuan Terintegrasi Dengan Satuan Siber,

- Tujuannya, untuk memadukan seluruh sistem jaringan yang ada di satuan dengan satuan siber, agar terciptanya suatu kendali monitoring dan penga mananjaringan secara terpusat.
- Metode yang digunakan dalam strategi ini adalah dengan membuat suatu konfigu

rasi pada perangkat jaringan yang ter dapat di satuan kerja Mabesau, Kotama dan Lanud. Adapun grand design sistem satuan jaringan terintegrasi dengan satuan Siber sebagai berikut:

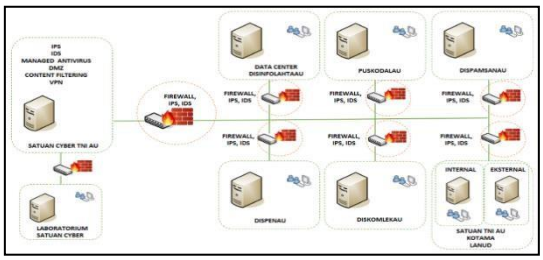
Gambar 6.1 Grand Design Konfigurasi Satuan dengan Satuan Siber



Strategi Mengatasi ancaman virus

- Tujuannya, untuk memastikan seluruh sistem pengamanan jaringan yang sudah tergelar aman dari virus.
- Metode yang digunakan dalam strategiini adalah dengan memberikan antivirus pada perangkat jaringan, server, dan client. Adapun sistem jaringan yang dapat mengatasi ancaman virus dapat digambar sebagai berikut:

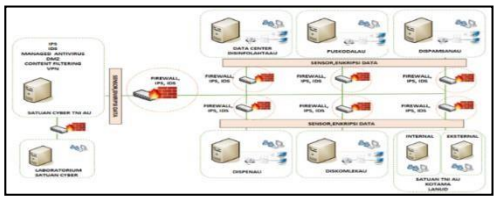
Gambar 6.2 Grand Design Instalasi Antivius Jaringan pada Server dan Client



Strategi Meningkatkan sistempertahanan jaringan

- Tujuannya, untuk meningkatkan sistem pengamanan jaringan yang sudahtergelar.

Gambar 6.3 Grand Design Instalasi Sistem Pertahanan Jaringan

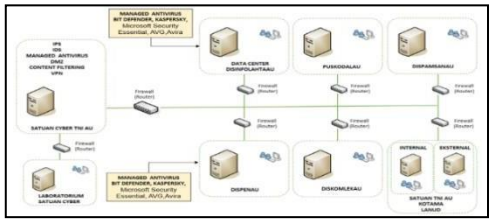


Strategi Interkoneksi

- Tujuannya, untuk memastikan seluruh sistem pengamanan jaringan yang sudah tergelar komunikasi data dan informasinya terhindar dari gangguan dan ancaman pencurian, sehingga data dan informasi yang melalui jaringan dapat berjalan dengan aman dan lancar.
- Metode, yang digunakan dalam strategi ini adalah dengan membuat suatu teknik pengamanan data. Cara kerja enkripsi dilakukan dengan menambahkan kode karakter teks sumber dengan teks kunci. Kunci yan lebih pendek dari teks sumber akan berulang-ulang sampai panjangnya sama dengan teks sumber. Teknik pengamanan ini terhubung langsung pada jaringan kemudian di proses oleh server atau router, hal ini dapat dilihat seperti gambar di bawah ini.

Gambar 6.4 Grand Design Pengamanan Data

pada Jaringan dengan Enkripsi



5. KESIMPULAN

- Metode, yang digunakan dalam strategi ini adalah dengan meng instalasi perangkat jaringan berupa hardware dan software. Sistem penga wasan jaringan diinstalasi pada perangkat dan server menggunakan IPS, IDS dan Firewall sebagai peng halang masuknya user yang tidak mendapatkan ijin akses dalam jaringan. Gambaran tentang metode ini dapat dilihat pada gambar berikut:
- Satuan siber TNI AU bertugas melaksanakan penangkalan untuk melin dungi infrastruktur informasi kritis TNI, yang meliputi aplikasi, sistem komputer dan jaringan dari berbagai macam dimensi ancaman ataupun serangan siber. Namun kondisi saat ini satuan Siber belum berfungsi sebagai puskodal sistem penga manan komunikasi data dan jaringan di lingkungan TNI AU hal ini disebabkan karena belum terinte grasinya jaringan-jaringan di satuan TNI AU dengan Satuan Siber. Selain itu, sistem operasi masih rentan terhadap kerusakan yang disebab

kan oleh virus dan sistem jaringan masih rentan terhadap ancaman Siber karena sistem keamanan jaringan masih lemah.

- Berdasarkan permasalahan tersebut maka diperlukan upaya-upaya untuk mengatasinya dengan melaksanakan konfigurasi untuk mengintegrasikan sistem jaringan satuan-satuan dengan satuan Siber, pengadaan anti virus untuk server dan client untuk mengantisipasi sistem operasi yang masih rentan terhadap kerusakan, instalasi dengan menjalankan prosedur pencegahan dan penangkalan serta pemulihan untuk sistem jaringan yang rentan oleh ancaman siber, kemudian melaksanakan enkripsi data dan pembuatan open VPN di jaringan internet untuk kerentanan pencurian data/ informasi akibat interkoneksi.

- Satuan terkait (*stakeholders*) saling berkoordinasi dan bekerja sama untuk menyiapkan personel yang mempunyai kapabilitas dalam penguasaan teknologi, khususnya teknologi jaringan untuk satuan siber sesuai DSP, mengakomodir dan memenuhi kebutuhan satuan siber berupa *bandwith* internet astinet dan VPN IP mulai dari tingkat Lanud jajaran, Kotama dan Mabesau serta menyediakan vendor yang memiliki kapasitas sebagai penyedia *hardware* dan *software* sistem pengama nan jaringan serta pihak vendor harus sesuai perjanjian yang tertuang dalam perjanjian MoU.
-

6. REFERENSI

Doktrin Siber Tentara Nasional Indonesia Nomor KEP/1355/XII/2018, LampiranC, Ancaman dan serangan Siber

Keputusan Kepala Staf Angkatan UdaraNomor Kep/722/XI/2016tentang Keamanan Sistem Informasi.

Mercer and Justine, 2010, Human Resource Management In Education. www.bps.go.id, diakses tanggal 15 April 2020.

Perkasau Nomor 24 tahun 2014 tentang POP Disinfolahtaau Pasal 3

Peraturan Menteri Pertahanan Republik tentangPedoman Pertahanan Siber.

SistemPertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia. Media Informasi Dirjend Pothan. Kemenrtrian Pertahanan RI

Undang-Undang RI Nomor 34 Tahun2004, Pasal 10.

.

.

Undang-Undang RI Nomor 3 Tahun 2002

tanggal 8 Januari 2002 tentangPertahanan Negara

Undang-Undang RI Nomor 34 Tahun 2004 tanggal 16 Oktober 2004 tentangTentara Nasional Indonesia

Undang-Undang ITE No. 19 Tahun 2016 tentang perubahan atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.