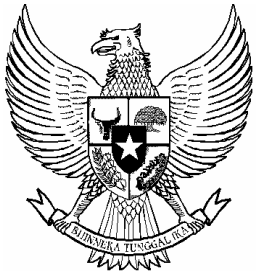


BERITA NEGARA REPUBLIK INDONESIA

No.1712, 2014 KEMENHAN. Pertahanan. Siber. Pedoman.

PERATURAN MENTERI PERTAHANAN REPUBLIK INDONESIA

NOMOR 82 TAHUN 2014

TENTANG

PEDOMAN PERTAHANAN SIBER

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI PERTAHANAN REPUBLIK INDONESIA,

Menimbang :

a. bahwa untuk menjabarkan Pedoman Strategis Pertahanan Nirmiliter perlu ditetapkan Pedoman Pertahanan Siber;

b. bahwa pedoman pertahanan siber merupakan acuan dasar bagi Kementerian Pertahanan/TNI dalam rangka penyelenggaraan pertahanan siber;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Menteri Pertahanan tentang Pedoman Pertahanan Siber;

Mengingat :

1. Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 3, Tambahan Lembaran Negara Republik Indonesia Nomor 4169;

2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843);

3. Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 166, Tambahan Lembaran Negara Republik Indonesia Nomor 4916);
4. Peraturan Menteri Pertahanan Nomor 25 Tahun 2014 tentang Doktrin Pertahanan Negara (Berita Negara Republik Indonesia Tahun 2014 Nomor 973);
5. Peraturan Menteri Pertahanan Nomor 57 Tahun 2014 tentang Pedoman Strategis Pertahanan Nirmiliter (Berita Negara Republik Indonesia Tahun 2014 Nomor ……);

MEMUTUSKAN:

Menetapkan : PERATURAN MENTERI PERTAHANAN TENTANG PEDOMAN PERTAHANAN SIBER

Pasal 1

Pedoman Pertahanan Siber sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

Pasal 2

Pedoman Pertahanan Siber sebagaimana dimaksud dalam Pasal 1 menjadi acuan dasar bagi Kementerian Pertahanan/TNI dalam rangka penyelenggaraan pertahanan siber.

Pasal 3

Peraturan Menteri ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Menteri ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 17 Oktober 2014
MENTERI PERTAHANAN
REPUBLIK INDONESIA,

PURNOMO YUSGIANTORO

Diundangkan di Jakarta
pada tanggal 17 Oktober 2014
MENTERI HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

AMIR SYAMSUDIN

PEDOMAN
PERTAHANAN SIBER

KEMENTERIAN PERTAHANAN REPUBLIK INDONESIA

2014

KATA PENGANTAR

Sistem pertahanan negara bersifat semesta melibatkan seluruh warga negara, wilayah, dan sumber daya nasional lainnya, serta dipersiapkan secara dini oleh pemerintah dan diselenggarakan secara total, terpadu, terarah, dan berlanjut untuk menegakkan kedaulatan negara, keutuhan wilayah, dan keselamatan segenap bangsa dari segala ancaman. Keterpaduan itu merujuk pada elemen kekuatan yang dibangun dalam sistem pertahanan semesta, yang memadukan kekuatan pertahanan militer dan kekuatan pertahanan nirmiliter.

Merujuk pada dasar Konstitusi, kekuatan pertahanan nirmiliter khususnya dalam ranah siber dibangun berdasarkan diktum upaya pembelaan negara, yang secara konseptual kekuatannya diserahkan kepada Kementerian/Lembaga Pemerintah Non Kementerian di luar bidang pertahanan, yaitu Kementerian Kominfo sebagai unsur utama dan Kementerian Pertahanan sebagai salah satu unsur dukungan bersama kekuatan bangsa lainnya. Mengingat luas bidang pertahanan siber itu, guna membangun *sense of defence* dalam bidang keamanan siber di sektor Pertahanan, perlu disusun Pedoman Pertahanan Siber.

Pedoman pertahanan siber ditetapkan sebagai pengejawantahan tekad, prinsip dan kehendak untuk menyelenggarakan pertahanan siber pada sistem informasi, kendali dan komunikasi di sektor pertahanan. Pedoman ini mewujudkan kerangka penyelenggaraan pertahanan siber yang harus dipahami dan dipedomani oleh sesuai tugas dan fungsi masing-masing. Dengan terbitnya Pedoman ini, seluruh pemangku kepentingan terkait hendaknya dapat menghayati dan mempedomani isinya, sehingga tampak dalam pola pikir, pola sikap dan pola tindak dalam menjamin keamanan jaringan dan muatannya di sektor pertahanan.

Saya selaku pimpinan Kementerian Pertahanan Republik Indonesia menyampaikan rasa syukur kepada Tuhan Yang Maha Esa atas terbitnya Pedoman Pertahanan Siber. Tidak lupa saya menyampaikan penghargaan dan ucapan terima kasih kepada semua pihak yang telah berperan serta dalam penyiapan Pedoman Pertahanan Siber ini. Saya yakin, peran serta tersebut merupakan dharma bhakti bagi Bangsa dan Negara Indonesia yang kita cintai.

Semoga Tuhan Yang Maha Esa senantiasa memberikan rahmat dan hidayah-Nya kepada kita semua.

Jakarta, 2014

Menteri Pertahanan,

Purnomo Yusgiantoro

RINGKASAN EKSEKUTIF

Pemanfaatan Teknologi Informasi dan Komunikasi (TIK), termasuk jaringan internet yang awalnya dibangun atas prakarsa Departemen Pertahanan Amerika Serikat sebagai sarana strategis komunikasi dan pertukaran data, telah semakin meluas memasuki semua sisi kehidupan manusia dewasa ini sebagai bagian sangat strategis kehidupan sosial, ekonomi dan bernegara di dunia. Hal yang sama juga berlaku di Indonesia yang pada saat ini memiliki jumlah penduduk seperempat milyar dan pertumbuhan pengguna internet yang tinggi dengan pertumbuhannya yang sangat pesat.

Ruang tempat berlangsungnya kegiatan pemanfaatan TIK dan internet ini disebut ruang siber. Ruang siber pada satu sisi membawa begitu banyak manfaat namun di sisi lain juga dapat memunculkan berbagai ancaman dan potensi serta gangguan mulai dari skala kecil hingga skala yang besar. Hal ini menyebabkan pentingnya diupayakan penjagaan kerahasiaan, integritas dan ketersediaan informasi elektronik serta infrastrukur di ruang siber tersebut agar terselenggara dengan tepat, yang ini dikenal sebagai pertahanan siber atau "*cyber defense*".

Penerapan pertahanan siber menjadi keniscayaan dan merupakan suatu prioritas kewajiban bagi negara dan semua instansi di dalamnya dimana tingkat pentingnya berbanding lurus dengan tingkat ketergantungan pada pemanfaatan di ruang siber tersebut. Hal ini menyebabkan Kemhan/TNI berkewajiban untuk mengambil langkah-langkah penting terkait dengan pertahanan siber, baik di dalam lingkungannya sendiri maupun dalam rangka mendukung pertahanan siber lintas sektoral. Pertahanan siber perlu dilaksanakan secara terencana dan terpadu agar penerapannya dapat berjalan secara tepat dan optimal. Untuk itu, disusunlah satu Pedoman Pertahanan Siber.

Penyusunan pedoman ini dilakukan dengan mengacu pada naskah kajian Peta Jalan Strategi Nasional Pertahanan Siber, yang berisi uraian lengkap mengenai ancaman dan serangan siber termasuk analisisnya terhadap strategi pertahanan siber yang telah pula mengakomodasikan perbandingan pertahanan siber di negara-negara lain.

Pedoman Pertahanan Siber ini mengurai kondisi saat ini di lingkungan termasuk upaya yang sudah dan sedang dilaksanakan. Untuk memudahkan pemahaman sistematika penulisannya, pedoman ini dibagi dalam; unsur kebijakan, kelembagaan, teknologi/infratruktur dan sumber daya manusia. Keempat unsur tersebut perlu mendapat perhatian yang seimbang sebagai persyaratan utama bagi berjalannya pertahanan siber yang komprehensif dan holistik. Pedoman ini menjelaskan langkah-langkah penyelenggaraan pertahanan siber serta tahapan penerapannya

karena persiapan masing-masing unsur tersebut sangat memerlukan waktu dan sumber daya yang tidak sedikit.

Akhirnya, pedoman ini diharapkan dapat menjadi acuan utama bagi perencanaan, pembangunan, pengembangan, penerapan dan evaluasi penyelenggaraan pertahanan siber di lingkungan Kemhan/TNI. Memperhatikan dinamika teknologi terkait ruang siber serta kondisi bangsa dan negara maka dari waktu ke waktu pedoman ini perlu ditinjau kembali agar dapat tetap sesuai dengan kondisi dan kebutuhan yang ada di lingkungan Kemhan/TNI.

DAFTAR ISI

Pengantar i

Ringkasan Eksekutif iii

Daftar Isi v

BAB I PENDAHULUAN 1

1.1. Latar Belakang 1

1.2. Maksud dan Tujuan 3

1.3. Ruang Lingkup 4

1.4. Landasan Hukum 4

1.5. Pengertian 5

BAB II URGENSI PERTAHANAN SIBER 6

2.1. Umum 6

2.2. Ancaman dan Serangan Siber 6

a. Ancaman Siber 6

b. Serangan Siber 12

2.3. Kondisi Saat Ini 15

2.4. Kebutuhan Pertahanan Siber 16

BAB III POKOK POKOK PERTAHANAN SIBER 18

3.1. Umum 18

3.2. Prinsip Prinsip Pertahanan Siber 18

3.3. Sasaran Pertahanan Siber 19

3.4. Tugas, Peran dan Fungsi Pertahanan Siber 20

a. Tugas Pertahanan Siber 20

b. Peran Pertahanan Siber 20

c. Fungsi Pertahanan Siber 21

BAB IV PENYELENGGARAAN PERTAHANAN SIBER 22

4.1. Umum 22

4.2. Kerangka Kerja Penyelenggaraan Pertahanan Siber..... 22

a. Kebijakan/Regulasi..... 23

b. Kelembagaan/Organisasi 33

c. Teknologi/Infrastruktur 34

d. Sumber Daya Manusia 34

4.3. Tahapan Penyelenggaraan Pertahanan Siber .. 39

a. Tahap Pencegahan Serangan..... 39

b. Tahap Pemantauan Pengamanan Informasi 40

c. Tahap Analisis Serangan 40

d. Tahap Pertahanan 41

e. Tahap Serangan Balik 41

f. Tahap Peningkatan Pengamanan Informasi 41

4.4. Pentahapan Kegiatan Pertahanan Siber..... 42

a. Tahap Persiapan..... 42

b. Tahap Pematangan 43

c. Tahap Pemanfaatan..... 46

d. Tahap Optimalisasi..... 48

BAB V PENUTUP 50

Daftar Pustaka 51

LAMPIRAN I Rancangan Awal Struktur Organisasi 52

LAMPIRAN II Rancangan Umum Spesifikasi Teknis Teknologi dan Infrastruktur Pertahanan Siber... 54

LAMPIRAN III Siklus Pertahanan Siber 63

BAB I

PENDAHULUAN

1.1. Latar Belakang

Pemanfaatan Teknologi Informasi dan Komunikasi (TIK) pada saat ini sudah memasuki semua aspek kehidupan masyarakat di dunia. Pemanfaatan TIK tersebut mendorong terbentuknya satu komunitas yang terhubung secara elektronik dalam satu ruang yang sering disebut ruang siber (*cyber space*). Sistem elektronik termasuk jaringan internet pada saat ini dimanfaatkan untuk mendukung berbagai kegiatan di sektor usaha, perdagangan, layanan kesehatan, komunikasi dan kepemerintahan, serta sektor pertahanan. Semakin meluasnya dan meningkatnya pemanfaatan TIK khususnya melalui jaringan internet diiringi pula dengan meningkatnya aktivitas ancaman. Ancaman itu antara lain upaya membobol kerahasiaan informasi, merusak sistem elektronik dan berbagai perbuatan melawan hukum lainnya.

Dengan memperhatikan hal di atas, ruang siber perlu mendapatkan perlindungan yang layak guna menghindari potensi yang dapat merugikan pribadi, organisasi bahkan negara. Istilah pertahanan siber muncul sebagai upaya untuk melindungi diri dari ancaman dan gangguan tersebut.

Pertahanan siber bertingkat dari lingkup perorangan, kelompok kerja, organisasi sampai dengan skala nasional. Perhatian yang khusus diberikan pada sektor yang mengelola infrastruktur kritis seperti pertahanan keamanan, energi, transportasi, sistem keuangan, dan berbagai layanan publik lainnya. Gangguan pada sistem elektronik pada sektor-sektor ini bisa menyebabkan kerugian ekonomi, turunnya tingkat kepercayaan kepada pemerintah, terganggunya ketertiban umum dan lain lain. Resiko ini yang menjadi pertimbangan diperlukannya pertahanan siber yang kuat dalam satu negara.

Sebagai instansi pemerintah, 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. Oleh karenanya Kemhan/TNI perlu mengambil langkah langkah persiapan untuk dapat menjalankan perannya dalam pertahanan siber sebagaimana diuraikan di atas.

Pedoman ini disusun untuk menjadi acuan bagi tahapan persiapan, pembangunan, pelaksanaan dan pemantapan pertahanan siber di lingkungan Kemhan/TNI. Acuan yang disusun meliputi aspek kebijakan, kelembagaan, teknologi/infrastruktur dan sumber daya

manusia. Setiap aspek tersebut sama penting dan bersifat saling mendukung sehingga memerlukan perhatian dari semua pihak yang terkait dengan pertahanan siber sesuai dengan peran dan tanggung jawabnya.

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.

Di dalam Undang-Undang RI Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dijelaskan bahwa pemanfaatan teknologi informasi membutuhkan pengamanan dalam rangka menjaga kerahasiaan, keutuhan dan ketersediaan informasi. Dalam Undang-undang tersebut, informasi dalam bentuk elektronik diakui secara hukum dan perbuatan yang terkait dengan sistem elektronik, baik selaku penyelenggara maupun selaku pengguna memiliki pertanggungjawaban hukum yang selanjutnya diatur dalam berbagai peraturan perundangan.

Kementerian Komunikasi dan Informatika RI, selaku *leading sector* Pemerintah RI dalam bidang Telekomunikasi dan Informatika memiliki 5 agenda kebijakan keamanan siber dalam membangun *Secure Cyber Environment*, melalui penerapan model strategi "*Ends-Ways-Means"* yang fokus pada sasaran, prioritas dan aksi yang terukur. Kelima kebijakan tersebut adalah: *Capacity Building, Policy* and *Legal Framework*, *Organizational Structure*, *Technical and Operational Measures, dan International Cooperation*. Selanjutnya peran Kementerian Komunikasi dan Informatika sebagai pengelola keamanan siber nasional dan kebijakan yang ditetapkannya dalam peran tersebut akan menjadi acuan utama bagi perumusan pedoman pertahanan siber ini.

Dihadapkan dengan kepentingan nasional, Kementerian Pertahanan RI sangat perlu untuk memahami, mengkaji, mengukur, mengantisipasi dan menyiapkan tindakan yang dibutuhkan. Oleh karena itu Kemhan/TNI perlu menyusun suatu pedoman pertahanan siber sebagai acuan yang digunakan untuk persiapan, pembangunan, pengembangan dan penerapan pertahanan siber di lingkungan Kemhan/TNI.

1.2. Maksud dan Tujuan

Pedoman ini dibuat dengan maksud sebagai acuan bagi Kemhan/TNI dalam rangka pertahanan siber guna mendukung kekuatan pertahanan negara, dengan tujuan untuk digunakan sebagai referensi utama dalam pembangunan, pengembangan dan penerapan pertahanan siber di lingkungan Kemhan/TNI.

1.3 Ruang Lingkup

Ruang lingkup pedoman pertahanan siber ini meliputi hal-hal sebagai berikut :

a. Konsep dasar pertahanan siber, meliputi latar belakang, landasan hukum dan pengertian.

b. Uraian mengenai pokok-pokok pertahanan siber, meliputi prinsip-prinsip, sasaran, ancaman dan serangan siber.

c. Perumusan kebutuhan pertahanan siber.

d. Penyelenggaraan Pertahanan Siber dan tahapan implementasinya.

1.4. Landasan Hukum

a. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, pasal 30 ayat 1, 2, dan 5 tentang Pertahanan dan Keamanan Negara.

b. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

c. Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara.

d. Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia.

e. Undang-Undang RI Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

f. Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik.

g. Undang-Undang Nomor 25 Tahun 2009 Tentang Pelayanan Publik.

h. Peraturan Menteri Pertahanan Nomor 57 Tahun 2014 tentang Pedoman Strategis Pertahanan Nirmiliter.

1.5. Pengertian

a. Ruang siber (*cyberspace*) atau siber adalah ruang dimana komunitas saling terhubung menggunakan jaringan (misalnya

internet) untuk melakukan berbagai kegiatan sehari-hari.

b. 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.

c. Keamanan Siber Nasional (*National cyber security*) adalah segala upaya dalam rangka menjaga kerahasiaan, keutuhan dan ketersediaan informasi serta seluruh sarana pendukungnya di tingkat nasional, yang bersifat lintas sektor.

d. Pertahanan siber (*cyber defense*) adalah suatu upaya untuk menanggulangi serangan siber yang menyebabkan terjadinya gangguan terhadap penyelenggaraan pertahanan negara.

e. Pedoman Pertahanan Siber adalah panduan dan/atau acuan yang digunakan untuk persiapan, pembangunan, pengembangan dan penerapan pertahanan siber di lingkungan Kemhan/TNI.

f. Infrastruktur kritis adalah aset, sistem, maupun jaringan, berbentuk fisik maupun virtual yang sangat vital, dimana gangguan terhadapnya berpotensi mengancam keamanan, kestabilan perekonomian nasional, keselamatan dan kesehatan masyarakat atau gabungan diantaranya.

BAB II

URGENSI PERTAHANAN SIBER

2.1. Umum

Urgensi pertahanan siber ditujukan untuk mengantisipasi datangnya ancaman ancaman dan serangan siber yang terjadi dan menjelaskan posisi ketahanan saat ini, sehingga diperlukan kesiapan dan ketanggapan dalam menghadapi ancaman serta memiliki kemampuan untuk memulihkan akibat dampak serangan yang terjadi di ranah siber.

2.2. Ancaman dan Serangan Siber

a. Ancaman Siber

1) Sumber Ancaman

Sumber Ancaman adalah entitas yang berkeinginan atau memiliki niat dan benar-benar secara nyata akan melakukan kegiatan yang melanggar norma dan hukum, aturan dan ketentuan serta kaidah atau kontrol keamanan informasi serta aset fisik lainnya, dengan tujuan untuk mendapatkan keuntungan yang bersifat materil dan immateril. Ancaman dan serangan tersebut dapat dilakukan oleh pelaku yang mewakili pemerintah (*State Actor*) atau non pemerintah (*Non State Actor*), sehingga pelaku bisa bersifat perorangan, kelompok, golongan, organisasi atau bahkan sebuah negara. Secara umum unsur-unsur yang dapat diidentifikasi memiliki potensi sebagai sumber ancaman terdiri atas :

a) Sumber Internal dan Eksternal.

b) Kegiatan Intelijen.

c) Kekecewaan.

d) Investigasi.

e) Organisasi Ekstremis.

f) Hacktivists.

g) Grup Kejahatan Terorganisir.

h) Persaingan, Permusuhan & Konflik.

i) Teknologi.

2) Aspek Ancaman

Aspek ancaman adalah segala sesuatu yang melatarbelakangi terjadinya ancaman dan serangan siber, yang meliputi aspek-aspek Ideologi, Politik, Ekonomi, Sosial, Budaya, Kebangsaan,

Militer, Ilmu Pengetahuan dan Teknologi serta aspek lain yang terkait dalam kehidupan berbangsa, bernegara dan bermasyarakat termasuk kepentingan pribadi.

3) Bentuk Ancaman

Bentuk ancaman siber yang sering terjadi saat ini dapat berupa hal-hal sebagai berikut :

a) 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.

b) Serangan *Defacement*, dilakukan dengan cara melakukan penggantian atau modifikasi terhadap halaman web korban sehingga isi dari halaman web korban berubah sesuai dengan motif penyerang.

c) 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.

d) 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.

e) 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 :

(1) 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.

(2) *Account* yang tidak terlindungi. Pengguna juga dapat melakukan kesalahan, dengan tidak memasang *password* atau dengan mudah memberikan *password* kepada orang lain.

(3) 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.

(4) 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.*

(5) *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.

(6) 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.

(7) *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.

(8) 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.

f) *Spam*. Spam adalah pengiriman *e-mail* secara massal yang tidak dikehendaki, dengan tujuan :

(1) Komersial atau publisitas.

(2) Memperkenalkan perangkat lunak berbahaya, seperti *malware* dan *crimeware* ke dalam sistem.

(3) Pada situasi terburuk, *spam* menyerupai serangan bom *e-mail*, dengan akibat *mail server* mengalami kelebihan beban, *mailbox user* penuh dan ketidaknyamanan dalam pengelolaan. Sebelumnya *spam* hanya dianggap sebagai gangguan, tapi saat ini *e-mail* spam merupakan ancaman nyata. Hal tersebut telah menjadi vektor istimewa untuk penyebaran virus, *worm, trojans, spyware* dan upaya *phishing*.

g) Penyalahgunaan Protokol Komunikasi. Sebuah serangan s*poofing 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*.

4) Jenis Ancaman

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

a) 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*.

b) 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.

c) 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.

b. Serangan Siber

1) Serangan Siber (*Cyber Attack*) terjadi ketika intensitas dan skala ancaman siber meningkat dan berubah dari ancaman yang bersifat potensial menjadi faktual berupa kegiatan atau tindakan yang bertujuan untuk memasuki, menguasai, memodifikasi, mencuri atau merusak, atau menghancurkan atau melumpuhkan sistem atau aset informasi, yang dikategorikan, sebagai berikut :

a) Perang Siber (*Cyber war*), adalah semua tindakan yang dilakukan secara sengaja dan terkoordinasi dengan tujuan mengganggu kedaulatan negara. Perang siber dapat berupa serangan terorisme (*cyber terrorism*) maupun spionase (*cyber espionage*) yang mengganggu keamanan nasional. Adapun serangan siber memiliki karakteristik sebagai berikut :

(1) *Intentional* (disengaja).

(2) Kegiatan aktif.

(3) Skala besar.

b) Gangguan Siber (*Cyber Violence*), adalah serangan siber yang memiliki karakteristik sebagai berikut :

(1) *Unintentional* (Tidak disengaja).

(2) Kegiatan pasif.

(3) Skala kecil.

2) Penanggulangan Serangan Siber

Kegiatan penanggulangan serangan siber menggunakan pendekatan yang menyesuaikan diri dengan sumber dan bentuk serangan yang dihadapi. Bentuk penanggulangan serangan siber yang dilakukan dapat berupa :

a) Pertahanan siber (*cyber defense*), adalah suatu upaya untuk menanggulangi serangan siber yang menyebabkan terjadinya gangguan terhadap penyelenggaraan negara secara normal. Pertahanan siber disiapkan sebagai suatu upaya penanggulangan serangan siber semacam ini.

b) Penanganan secara hukum. Melakukan koordinasi dengan aparat keamanan terkait apabila telah diketahui pelaku kejahatan siber.

c) Serangan balik siber (*Cyber counter-attack*), adalah suatu tindakan serangan balik terhadap sumber serangan dengan tujuan memberikan efek jera terhadap pelaku serangan siber.

3) Sasaran Serangan Siber

Berdasarkan tujuan dan sasarannya, serangan siber ditujukan kepada :

a) Perorangan, masyarakat umum, organisasi, komunitas tertentu, yang bersifat kejahatan siber.

b) Obyek Vital Infrastruktur Kritis Nasional (*National Critical*

Infrastructure), yaitu sistem-sistem infrastruktur fisik yang sangat penting dimana bila sistem ini tidak berfungsi atau rusak, maka dapat berdampak melemahkan pertahanan atau keamanan serta ekonomi bangsa.

c) Kepentingan nasional, yaitu seluruh aspek yang terkait dengan tujuan nasional, lambang / simbol negara, politik negara serta kepentingan bangsa.

4) Dampak Serangan Siber

Dampak yang mungkin dialami dari sebuah serangan siber dapat berbentuk :

a) Gangguan fungsional.

b) Pengendalian sistem secara *remote*.

c) Penyalahgunaan informasi.

d) Kerusuhan, ketakutan, kekerasan, kekacauan, konflik.

e) Serta kondisi lain yang sangat merugikan, sehingga memungkinkan dapat mengakibatkan kehancuran.

2.3. Kondisi Saat Ini

Kondisi Pertahanan Siber saat ini di lingkungan Kemhan/TNI dapat diuraikan sebagai berikut :

a. Kebijakan

Kebijakan untuk pertahanan siber sudah mulai disusun dan pelaksanaannya dilakukan pada tahapan berikutnya. Kebijakan tersebut melengkapi kebijakan yang ada, yang pada umumnya masih fokus pada pengembangan dan pemanfaatan teknologi informasi di lingkungan Kementerian secara umum. Salah satu kebijakan pijakan yang ada adalah Peraturan Menhan Nomor 16/2010 tentang Organisasi dan Tatakerja Kemhan, yang salah satunya menguraikan peranan dari Pusdatin Kemhan dan Unit-unit Datin di Satker Kemhan. Selain itu telah disusun pula kebijakan yang diperlukan dalam menunjang pertahanan siber. Kebijakan tersebut pada masa yang akan datang akan menjadi acuan bagi persiapan, pengembangan, pelatihan dan pengoperasian pertahanan siber.

b. Kelembagaan

Sebagaimana diuraikan dalam butir a, kelembagaan pada saat ini masih bersifat mendukung teknologi informasi secara umum dan belum mendukung keperluan pertahanan siber yang lebih spesifik. Langkah-langkah pembentukan kelembagaan pertahanan siber sudah mulai diambil, tetapi

masih dalam bentuk penambahan tugas dan fungsi pertahanan siber ke dalam struktur yang ada.

c. Teknologi dan Infrastruktur pendukung

Teknologi dan Infrastruktur pendukung yang tersedia saat ini baik yang bersifat umum maupun khusus menunjang pertahanan siber, masih dalam proses peningkatan.

d. Sumber Daya Manusia

Persiapan untuk penyediaan SDM dalam rangka mendukung pertahanan siber sudah mulai dilakukan, meskipun baru persiapan awal dalam bentuk program peningkatan kesadaran (*awareness*) dan peningkatan pengetahuan dan ketrampilan keamanan informasi. Implementasi Pertahanan siber pada masa yang akan datang akan memerlukan program peningkatan SDM yang jauh lebih besar dan substantif.

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. Memperhatikan dua kepentingan tersebut maka diperlukan antisipasi bagi kebutuhan pertahanan siber yang meliputi aspek-aspek :

a. Kebijakan

Kebijakan-kebijakan yang menjadi acuan bagi seluruh kegiatan pertahanan siber termasuk pengembangan, pengoperasian dan koordinasi sangat penting untuk dirumuskan dan ditetapkan. Kebijakan-kebijakan ini meliputi aspek pengembangan kelembagaan, persiapan infrastruktur dan teknologi, persiapan Sumber Daya Manusia dan penetapan peran, fungsi dan wewenang dalam pertahanan siber di lingkungan Kemhan/TNI. Kebutuhan ini perlu diwujudkan dalam bentuk peraturan, pedoman, petunjuk teknis dan bentuk-bentuk kebijakan lain yang dapat memastikan kegiatan pertahanan siber dapat berjalan sebagaimana mestinya.

b. Kelembagaan

Kelembagaan yang kuat dan efektif sangat diperlukan dalam menjalankan tugas-tugas dan kegiatan pertahanan siber, dengan mengacu kepada kebijakan yang ditetapkan. Hal ini meliputi struktur organisasi, pembagian tugas dan wewenang, dan mekanisme kerja serta pengawasan. Kelembagaan ini perlu

diwujudkan melalui kajian pengembangan kelembagaan di seluruh satker Kemhan/TNI yang diikuti dengan langkah-langkah persiapan, dan pembentukan, penyesuaian dan/atau penguatan kelembagaan sehingga tersedia kelembagaan yang efektif dalam mendukung pertahanan siber.

c. Teknologi dan Infrastruktur pendukung

Teknologi dan infrastruktur pendukung yang lengkap, diperlukan sebagai sarana dan kelengkapan bagi kegiatan pertahanan siber yang diselenggarakan, agar pertahanan siber dapat terlaksana dengan efektif dan efisien. Teknologi dan infrastruktur pendukung ini perlu diwujudkan melalui kajian pengembangan yang diikuti dengan langkah-langkah persiapan, dan pembentukan, penyesuaian dan/atau penguatan teknologi dan infrastruktur yang dapat dimanfaatkan secara maksimal dalam memenuhi kebutuhan pertahanan siber.

d. Sumber Daya Manusia

Sumber Daya Manusia merupakan satu unsur yang terpenting dalam memastikan terlaksananya pertahanan siber sesuai dengan kebijakan-kebijakan yang ditetapkan. Pengetahuan dan ketrampilan khusus pertahanan siber harus dimiliki dan dipelihara sesuai dengan perkembangan kondisi kebutuhan pertahanan siber. Sumber Daya Manusia diwujudkan dalam bentuk program rekruitmen, pembinaan serta pemisahan yang mengacu pada ketentuan yang berlaku.

BAB III

POKOK-POKOK PERTAHANAN SIBER

3.1. Umum

Dalam rangka persiapan, pembangunan, pengembangan dan penerapan pertahanan siber di lingkungan Kemhan/TNI, diperlukan persamaan pemahaman tentang prinsip-prinsip, sasaran serta tugas, peran dan fungsi pertahanan siber yang akan dilaksanakan. Hal ini menjadi acuan dalam penetapan resiko yang ditimbulkan sehingga menentukan langkah-langkah pertahanan siber yang akan diambil.

3.2. Prinsip-prinsip Pertahanan Siber

a. Memiliki model pengamanan informasi yang terstruktur dan terintegrasi serta mengadopsi berbagai standar dan panduan pengamanan informasi yang ditetapkan oleh institusi yang berwenang.

b. Faktor kerahasiaan, integritas dan ketersediaan pertahanan siber harus dipastikan sejak tahap perancangan sebagai salah satu prinsip dasar keamanan informasi.

c. Pertahanan siber mengandung unsur kebijakan, kelembagaan, teknologi dan infrastruktur pendukung serta Sumber Daya Manusia.

d. Implementasi pertahanan siber harus dilakukan oleh SDM yang memiliki kompetensi, integritas yang tinggi dan terlindungi.

e. Dilakukan secara efektif dan efisien dalam bentuk keamanan fisik dan keamanan logis secara terintegrasi dengan memanfaatkan semaksimal mungkin teknologi terbuka dan produk Indonesia dalam rangka kemandirian dan kedaulatan.

f. Penetapan zona pengamanan berdasarkan klasifikasi SDM yang terlibat seperti *administrator*, pengguna dan tipe lain.

g. Mengacu kepada prinsip-prinsip tata kelola yang menjamin terwujudnya pengawasan melekat dalam pertahanan siber.

h. Menjamin bahwa implementasi sistem siber aman dan tahan terhadap serangan siber lawan

i. Mengembangkan kondisi yang lebih menguntungkan untuk tindakan ofensif.

j. Menghindari kerugian pada sistem komputer yang tidak diinginkan.

3.3.Sasaran Pertahanan Siber.

Sasaran yang hendak dicapai pedoman ini adalah :

a. Terdapatnya pemahaman atas situasi dan kondisi terkini menyangkut ancaman dan serangan siber khususnya dalam sektor pertahanan termasuk penanganannya baik di dalam dan luar negeri.

b. Terbangunnya kesadaran (*awareness*) akan arti penting pertahanan siber dalam rangka pengamanan sumber daya informasi khususnya sektor pertahanan dan secara umum bagi infrastruktur kritis nasional.

c. Terlibatnya semua pihak terkait secara penuh dan terpadu dalam inisiatif pertahanan siber di lingkungan Kemhan/TNI.

d. Terbangunnya potensi sumber daya dalam pengembangan pertahanan siber sebagai bagian dari sistem pertahanan negara.

e. Terumuskannya strategi penangkalan, penindakan dan pemulihan bidang pertahanan siber.

f. Tersedianya acuan bagi penyediaan fasilitas, sarana dan prasarana serta pengetahuan dan ketrampilan guna mendukung langkah langkah persiapan, pembangunan, pengembangan dan penerapan pertahanan siber.

3.4. Tugas, Peran dan Fungsi Pertahanan Siber.

Dalam rangka memastikan pertahanan siber dapat dijalankan secara baik, maka diperlukan dukungan kelembagaan yang kuat, profesional dan andal untuk memastikan tujuan dari pertahanan siber dapat tercapai. Kegiatan pengorganisasian ini diharapkan dapat mewujudkan peran dan fungsi sebagai integrator, inisiator, koordinator dan mediator dari seluruh kegiatan pengamanan informasi di lingkungan Kementerian Pertahanan dan TNI.

a. Tugas Pertahanan Siber.

1) Menjamin terwujudnya ketahanan siber di lingkungan Kemhan dan TNI.

2) Menjaga sumber daya informasi Kemhan/TNI agar terlindung dari gangguan dan penyalahgunaan atau pemanfaatan pihak-pihak lain;

3) Menjaga keamanan informasi infrastruktur kritis TIK Kemhan/TNI;

4) Mendorong partisipasi aktif pemanfaatan ruang siber yang aman melalui kerjasama kemitraan nasional dan

internasional lintas sektoral;

5) Membangun kapasitas pertahanan siber berupa kemampuan penangkalan, penindakan dan pemulihan; dan

6) Menyelenggarakan dan mengembangkan pengelolaan kelembagaan Pertahanan Siber yang bertanggung jawab, efektif, efisien dan akuntabel;

b. Peran Pertahanan Siber.

1) Sebagai Jaringan Data Antara Satuan jajaran Yang Aman. Hal ini dilakukan untuk menjaga keamanan jaringan strategis antara lembaga dalam upaya menjaga kerahasiaan dan ketersediaan / keberlangsungan jaringan yang diterapkan secara konsisten pada semua lembaga terkait.

2) Sebagai Model Pusat Data dan Sarana Pendukung Yang Aman. Hal ini dilakukan untuk menjaga keamanan informasi strategis yang dapat menjadi contoh/acuan bagi semua lembaga. Model Pusat Data dan Sarana pendukung harus memberi acuan yang memperhatikan:

(a) Pemanfaatan teknologi tepat guna (*usability*)

(b) Kemampuan pengelolaan dan pengoperasian yang efisien dan mandiri (*manageability*)

(c) Kemampuan pengembangan lebih lanjut (*scalability*)

c. Fungsi Pertahanan Siber.

1) Menjamin tercapainya sinergi kebijakan pertahanan siber.

2) Membangun organisasi dan tata kelola sistem penanganan keamanan siber.

3) Membangun sistem yang menjamin ketersediaan informasi dalam konteks pertahanan siber.

4) Membangun sistem penangkalan, penindakan dan pemulihan terhadap serangan siber.

5) Mewujudkan kesadaran keamanan siber.

6) Meningkatkan keamanan sistem siber sektor pertahanan.

7) Mewujudkan riset dan pengembangan untuk mendukung pembinaan dan pengembangan kemampuan Pertahanan Siber.

8) Menyelenggarakan kerjasama nasional dan internasional guna pembinaan dan pengembangan kemampuan Pertahanan Siber.

BAB IV

PENYELENGGARAAN PERTAHANAN SIBER

4.1. Umum

Pedoman pertahanan siber digunakan sebagai acuan di lingkungan Kemhan/TNI dalam rangka perencanaan, pembangunan pengembangan dan implementasi pertahanan siber. Selanjutnya dalam pedoman ini diuraikan persyaratan untuk masing-masing kebutuhan kebijakan, kelembagaan, teknologi/infrastruktur dan SDM.

Penangkalan, penindakan dan pemulihan dari ancaman siber tidak akan efektif jika tidak ada pengaturan kewenangan yang jelas. Dalam skala kompleksitas yang tinggi dalam penyelenggaraan pertahanan siber, pengaturan kewenangan dilakukan melalui optimalisasi masing-masing peran.

Pada satu eskalasi kejadian yang masuk dalam kategori luar biasa, koordinasi pelaksanaan pertahanan siber akan diatur melalui rujukan strategi pertahanan siber nasional. Hal ini memungkinkan Presiden selaku Kepala Negara mengambil tindakan yang diperlukan sesuai kewenangannya dalam mengelola sistem pertahanan negara, termasuk pertahanan siber. Kewenangan tersebut sesuai dengan kondisi dan kebutuhan dapat didelegasikan kepada Menteri Pertahanan atau pejabat lain.

4.2. Kerangka Kerja Penyelenggaraan Pertahanan Siber

Pengembangan, pembangunan dan implementasi pertahanan siber memerlukan kerangka kerja yang akan menjadi acuan agar implementasi dapat terjadi secara berkesinambungan dan dapat diukur kinerjanya setiap saat. Kebutuhan ini dipenuhi dengan pengembangan kerangka kerja yang meliputi kebijakan/regulasi, kelembagaan, teknologi dan SDM. Masing-masing bagian dari kerangka kerja tersebut diuraikan sebagai berikut :

a. Kebijakan/regulasi

Sesuai dengan tata kelola kepemerintahan yang baik (*good corporate governance*) yang menjadi fondasi pelaksanaan tugas-tugas instansi pemerintah, termasuk Kemhan/TNI, maka diperlukan kebijakan/regulasi sebagai landasan hukum. Kebijakan dan regulasi juga diperlukan untuk menjaga arah dari kegiatan-kegiatan pengembangan pembangunan dan penerapan pertahanan siber agar senantiasa sesuai dengan peraturan perundangan. Pada tingkatan operasional kebijakan regulasi berbentuk pedoman, petunjuk pelaksanaan, petunjuk teknis yang menjadi acuan utama bagi pertahanan siber. Tata cara

perumusan penetapan dan penerapan kebijakan pertahanan siber mengikuti tata cara berdasarkan peraturan perundangan dan dilakukan dengan mempertimbangkan kebutuhan nasional, perkembangan situasi dan kondisi pertahanan siber serta perkembangan teknologi.

1) Kebijakan dasar/pijakan untuk regulasi pertahanan siber
   a) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11/2008.
   b) Undang-Undang No. 3 Tahun 2002 tentang Pertahanan Negara.
   c) Peraturan Pemerintah Penyelenggara Sistem dan Transaksi Elektronik (PP PSTE) No. 82/2012.
   d) Peraturan Menhan Nomor 16 Tahun 2010 tentang Organisasi dan Tata Kerja Kemhan.
2) Kebijakan strategis pertahanan siber Kemhan/TNI
   a) Kebijakan umum pertahanan siber.
   b) Kebijakan kelembagaan pertahanan siber.
   c) Kebijakan pengembangan SDM pertahanan siber.
   d) Kebijakan pembangunan teknologi, pengembangan dan pemanfaatan infrastruktur pertahanan siber.
   e) Kebijakan kerjasama lintas sektor pertahanan siber.
   f) Kebijakan pembinaan potensi pertahanan siber.
   g) Kebijakan kerjasama luar negeri.
   h) Kebijakan pembangunan fasilitas dan sarana prasarana pendukung.
3) Kebijakan operasional penyelenggaraan pertahanan siber
   a) Perencanaan Keamanan Informasi (*Information Security Planning).*
   b) Tanggap Darurat (*Incident Response).*
   c) Manajemen resiko TIK (*IT Risk Management).*
   d) Pemulihan (*Disaster Recovery).*
   e) Rehabilitasi dan Rekonstruksi *(Disaster Rehabilitation and Reconstruction).*
   f) Manajemen Rekanan (*Vendor Management).*
   g) Operasi Jaringan *(Network Operations).*

h) Keamanan Sistem dan Aplikasi *(System and Application Security)*

i) Kontrol Akses (*Access Control).*

j) Kontrol Perubahan (*Change Control).*

k) Keamanan Fisik (*Physical Security).*

l) Klasifikasi data, penanganan dan pemusnahan (*Data Classification, Handling, and Disposal).*

m) Keamanan personel (*Personnel Security).*

n) Akses sistem dan penggunaan baku (*System Access and Acceptable Use).*

o) Privasi daring (*Online Privacy).*

p) Pelatihan dan kesadaran keamanan (*Security Training and Awareness).*

q) Asesmen diri (*Self Assessment).*

r) Metrik dan pengukuran keamanan (*Security Metrics and Measurement).*

s) Komputasi bergerak (*Mobile Computing).*

t) Keamanan Nirkabel (*Wireless Security).*

4) Manajemen Pengamanan Informasi di lingkungan Kemhan/TNI. Sistem ini merupakan bagian dari sistem manajemen secara keseluruhan yang menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan dan memelihara keamanan informasi berdasarkan pendekatan risiko. Sistem manajemen mencakup struktur, kebijakan, kegiatan perencanaan, tanggung jawab, praktek, prosedur, proses dan sumber daya organisasi.

a) Dalam manajemen pengamanan informasi, satker pelaksana bidang data dan informasi di lingkungan Kemhan/TNI harus melakukan hal-hal sebagai berikut :

(1) Menetapkan ruang lingkup dan batasan pengamanan informasi sesuai dengan tugas pokok, organisasi, lokasi, aset dan teknologi, termasuk rincian dari setiap pengecualian dan dasar justifikasi dari ruang lingkup.

(2) Menetapkan kebijakan pengamanan informasi sesuai dengan tugas pokok, organisasi, lokasi, aset dan teknologi yang :

(a) Mencakup kerangka kerja untuk menyusun

sasaran dan menetapkan arahan dan prinsip tindakan secara menyeluruh terkait dengan pengamanan informasi.

(b) Mempertimbangkan persyaratan berkaitan dengan hukum atau regulasi, serta kewajiban pengamanan informasi sesuai tugas pokok.

(c) Selaras dengan manajemen risiko strategis organisasi dalam konteks penetapan dan pemeliharaan pengamanan informasi yang akan dilaksanakan.

(d) Menetapkan kriteria terhadap risiko yang akan dievaluasi.

(e) Ditetapkan dengan Peraturan Kepala Badan/Dirjen atau lainnya sesuai struktur organisasi yang ada.

(3) Menetapkan pendekatan asesmen risiko pada organisasi dengan :

(a) Mengidentifikasi suatu metodologi asesmen risiko yang sesuai dengan manajemen pengamanan informasi, persyaratan hukum dan perundang-undangan yang berlaku.

(b) Mengembangkan kriteria untuk menerima risiko dan mengidentifikasi tingkat risiko yang dapat diterima. Metodologi asesmen risiko yang dipilih harus memastikan bahwa asesmen risiko memberikan hasil yang dapat dibandingkan dan direproduksi.

(4) Mengidentifikasi risiko, yaitu :

(a) Mengidentifikasi aset informasi dalam ruang lingkup manajemen pengamanan informasi dan kebijakan pimpinan.

(b) Mengidentifikasi ancaman-ancaman terhadap aset informasi.

(c) Mengidentifikasi kelemahan yang mungkin dieksploitasi oleh ancaman.

(d) Mengidentifikasi dampak hilangnya kerahasiaan, integritas dan ketersediaan dari aset informasi.

(5) Menganalisis dan mengevaluasi risiko yaitu :

(a) Menganalisis dampak yang mungkin berasal dari kegagalan pengamanan informasi, dengan mempertimbangkan konsekuensi hilangnya kerahasiaan, integritas atau ketersediaan aset informasi.

(b) Menganalisis kemungkinan terjadinya kegagalan pengamanan informasi yang realistik, berkenaan dengan ancaman dan kelemahan, dan dampak yang terkait dengan aset serta pengendalian yang diterapkan saat ini.

(c) Memperkirakan tingkat risiko.

(d) Menetapkan apakah risiko dapat diterima atau memerlukan perhatian lain.

(6) Mengidentifikasi dan mengevaluasi pilihan perlakuan risiko yang mencakup :

(a) Penerapan pengendalian yang tepat.

(b) Penerimaan risiko secara sadar dan objektif, jika risiko tersebut memenuhi kebijakan organisasi dan kriteria risiko yang dapat diterima.

(c) Pencegahan risiko.

(d) Pengalihan risiko kepada pihak lainnya seperti pihak asuransi atau pemasok.

(7) Memilih sasaran pengendalian dan pengendalian untuk perlakuan risiko. Sasaran pengendalian dan pengendalian harus dipilih dan diterapkan untuk memenuhi persyaratan yang diidentifikasi melalui proses asesmen risiko dan proses perlakuan risiko. Pemilihan ini harus mempertimbangkan kriteria risiko yang dapat diterima dan juga persyaratan hukum, perundang-undangan dan persyaratan lainnya.

(8) Memperoleh persetujuan pimpinan terhadap risiko residu yang diajukan.

(9) Menyiapkan pernyataan pemberlakuan yang mencakup :

(a) Sasaran pengendalian yang dipilih dan alasan-alasan pemilihannya.

(b) Sasaran pengendalian yang diterapkan saat ini.

(c) Pengecualian setiap sasaran pengendalian dan dasar untuk pengecualiannya.

b) Penerapan dan Pengoperasian Manajemen Pengamanan informasi. Dalam menerapkan dan mengoperasikan sistem manajemen ini, setiap satker harus melakukan hal-hal sebagai berikut :

(1) Merumuskan rencana perlakuan risiko yang mengidentifikasi tindakan manajemen sumber daya, tanggung jawab dan prioritas secara tepat untuk mengelola risiko pengamanan informasi.

(2) Menerapkan rencana perlakuan risiko untuk mencapai sasaran pengendalian yang teridentifikasi, yang mencakup pertimbangan pendanaan dan alokasi peran dan tanggung jawab.

(3) Menerapkan pengendalian yang dipilih untuk memenuhi sasaran pengendalian.

(4) Menetapkan bagaimana mengukur keefektifan pengendalian atau kelompok pengendalian yang dipilih dan menerangkan bagaimana pengukuran tersebut digunakan untuk mengakses keefektifan pengendalian untuk memperoleh hasil yang dapat dibandingkan dan direproduksi.

(5) Menerapkan program pelatihan dan kepedulian.

(6) Mengelola operasi dalam manajemen pengamanan informasi.

(7) Mengelola sumber daya untuk manajemen pengamanan informasi.

(8) Menerapkan prosedur dan pengendalian lainnya yang mampu melakukan deteksi secara cepat terhadap setiap kejadian dan insiden.

c) Memantau dan mengkaji Manajemen Pengamanan Informasi. Setiap satker pelaksana data dan informasi di lingkungan Kemhan/TNI harus melakukan hal-hal berikut :

(1) Melaksanakan prosedur pemantauan, pengkajian dan pengendalian lainnya untuk :

(a) Mendeteksi kesalahan hasil pengolahan secara cepat.

(b) Mengidentifikasi secara cepat terhadap pelanggaran dan insiden pengamanan informasi baik dalam bentuk upaya maupun yang telah berhasil.

(c) Memungkinkan pimpinan untuk menentukan apakah kegiatan pengamanan informasi didelegasikan kepada orang atau diterapkan dengan teknologi informasi yang dilaksanakan sebagaimana diharapkan.

(d) Membantu mendeteksi kejadian keamanan sehingga mencegah insiden keamanan dengan menggunakan indikator.

(e) Menentukan apakah tindakan-tindakan yang diambil untuk memecahkan masalah pelanggaran keamanan telah efektif.

(2) Melaksanakan tinjauan keefektifan manajemen pengamanan informasi dengan mempertimbangkan hasil audit pengamanan informasi, insiden, efektifitas, pendapat dan umpan balik dari semua pihak terkait.

(3) Mengukur keefektifan pengendalian pengamanan informasi.

(4) Mengkaji asesmen risiko pada interval yang direncanakan dengan mengkaji risiko residu dan tingkat risiko yang dapat diterima serta telah diidentifikasi dengan mempertimbangkan perubahan terhadap :

(a) Organisasi.

(b) Teknologi.

(c) Sasaran dan tata kelola.

(d) Ancaman yang diidentifikasi.

(e) Keefektifan dari pengendalian yang diterapkan.

(f) Kejadian eksternal seperti perubahan terhadap lingkungan hukum dan regulator, kewajiban kontrak yang berubah dan perubahan lingkungan sosial.

(5) Melaksanakan audit internal manajemen pengamanan informasi pada interval yang direncanakan, dimulai dari satker yang terkecil.

(6) Melaksanakan kajian manajemen pengamanan informasi secara reguler untuk memastikan bahwa ruang lingkup masih mencukupi dan peningkatan proses manajemen pengamanan informasi yang diidentifikasi.

(7) Memutakhirkan rencana pengamanan informasi dengan mempertimbangkan temuan dari kegiatan pemantauan dan pengkajian .

(8) Merekam tindakan dan kejadian yang dapat mempunyai dampak terhadap keefektifan atau kinerja manajemen pengamanan informasi.

d) Peningkatan dan Pemeliharaan Manajemen Pengamanan Informasi. Dalam peningkatan dan pemeliharaan sistem manajemen pengamanan informasi, organisasi harus melakukan secara reguler hal berikut :

(1) Menerapkan peningkatan yang diidentifikasi dalam manajemen pengamanan informasi.

(2) Mengambil tindakan korektif dan pencegahan yang tepat.

(3) Mengambil pelajaran dari pengalaman keamanan informasi organisasi lain.

(4) Mengkomunikasikan tindakan dan peningkatan kepada semua pihak yang terkait dengan tingkat rincian sesuai situasi dan kondisi, dan jika relevan, menyetujui tindak lanjutnya.

(5) Memastikan bahwa peningkatan tersebut mencapai sasaran yang dimaksudkan.

5) Standar yang menjadi acuan bagi kebijakan pertahanan siber. Dalam pengembangan dan penerapan pertahanan siber, kebijakan-kebijakan yang ada akan mengacu pada standar-standar nasional maupun internasional antara lain :

a) SNI (Standar Nasional Indonesia) *27001* tentang Sistem Manajemen Keamanan Informasi.

b) *ISO/IEC 20000 Information Technology Service Management System (ITSM).*

c) *ISO/IEC 22000 Business Continuity Management (BCM).*

d) *Control Objectives for Information and related Technology (COBIT).*

e) *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*.

f) *TIA-942 Data Center Standards.*

g) *Open Web Application Security Project (OWASP).*

h) *Open Source Security Testing Methodology Manual (OSSTMM).*

i) *Information Systems Security Assessment Framework (ISSAF).*

j) *National Institute of Standards and Technology (NIST) SP 800.*

b. Kelembagaan/Organisasi

Kelembagaan yang dibangun harus disesuaikan dengan kebutuhan penyelenggaraan pertahanan siber, guna memastikan tujuan dari pertahanan siber dapat tercapai secara optimal. Kelembagaan tersebut dapat dikembangkan tersendiri secara terpisah yang pada tahap awal dapat dipimpin pejabat setingkat Eselon II. Dalam penyusunan kelembagaannya harus dipenuhi persyaratan sebagai berikut :

1) Perumusan tugas dan fungsi yang lengkap dan jelas, sesuai dengan kebutuhan pertahanan siber. Pada tahap awal, rancangan struktur organisasi dituangkan pada lampiran I.

2) Kewenangan lembaga diuraikan jelas termasuk untuk melakukan koordinasi

3) Struktur organisasi efektif untuk mendukung spesialisasi dan pembagian peran agar SDM dapat fokus pada tugas masing masing.

4) Bentuk kelembagaan dapat bertahap sesuai kesiapan dan kebutuhan dari bentuk tim, satker, gugus tugas, struktural sampai dengan badan independen.

5) Ada kebijakan formal untuk menjadi dasar butir 1, 2, 3 dan 4 di atas.

c. Teknologi / Infrastruktur

Sesuai dengan ruang lingkup dan kewenangan serta skala prioritas, kelembagaan pertahanan siber memerlukan dukungan teknologi/infrastruktur sebagai berikut :

1) Sarana prasarana gedung/lokasi pusat data, *NOC*, laboratorium dan fasilitas pendukung lainnya.

2) Pusat Data dan pusat pemulihan (*Disaster Recovery Center*/*DRC*).

3) Jaringan Data.

4) Aplikasi administrasi pertahanan siber.

5) Aplikasi khusus teknis pertahanan siber.

6) Teknologi khusus (Perangkat keras dan perangkat lunak pendukung kegiatan spesifik pertahanan siber).

Rancangan umum spesifikasi teknis teknologi dan infrastruktur pertahanan siber dituangkan di lampiran II.

d. Sumber Daya Manusia

1) Aset utama dalam *cyber security* adalah personel atau SDM yang memainkan peran sangat penting dalam pertahanan siber. Tantangan terbesar dalam implementasi pertahanan siber adalah menyediakan SDM yang kompeten dan senantiasa cepat dan sigap mengikuti dinamika lingkungan siber yang terus berkembang seiring berkembangnya teknologi dan kondisi sosial masyarakat. Untuk itu strategi pengembangan SDM harus didukung dengan program peningkatan kompetensi yang berkesinambungan.

2) Agar dapat melaksanakan tugasnya dengan baik, maka beberapa persyaratan umum yang harus diperhatikan oleh lembaga pertahanan siber dalam pengembangan SDM adalah sebagai berikut :

a) Rekrutmen SDM. Proses ini harus melewati uji kesiapan mental melalui tes psikologi agar sesuai dengan profil dari SDM untuk pertahanan siber, seperti : harus dapat bekerja di bawah kondisi penuh tekanan, berintegritas tinggi, disiplin, memiliki kemampuan belajar dan lain-lain, sesuai dengan standar yang ditetapkan. Rekrutmen ini harus melalui kajian dan perlu ditinjau ulang secara berkala untuk mengakomodasi perkembangan situasi teknologi dan kebutuhan Pertahanan Siber Nasional. Kajian kebutuhan kompetensi ini meliputi ruang lingkup tugas, persyaratan pengetahuan dan ketrampilan yang harus dimiliki, persyaratan lain untuk memastikan adanya kemampuan untuk bekerja sesuai dengan kebutuhan pertahanan siber dan desain jenjang karir profesional yang terkait dalam Pertahanan Siber. Kajian kebutuhan kompetensi berkaitan erat dengan jenjang karir, yang digambarkan secara umum sebagai berikut :

b) SDM terpilih harus memiliki kompetensi sesuai dengan kebutuhan, dalam hal pengetahuan dan ketrampilan sesuai penempatan dan penugasan dalam pertahanan siber serta terjaminnya pembinaan karier SDM yang bersangkutan.

c) Untuk tugas-tugas khusus yang bersifat rahasia dan strategis, SDM terpilih harus memiliki status kepegawaian yang tidak menyalahi prinsip-prinsip organisasi pertahanan, khususnya untuk tugas yang bersifat ofensif atau dalam kondisi perang siber.

3) Pembinaan latihan dan peningkatan kemampuan SDM dapat dilakukan dengan cara sebagai berikut :

a) Program promosi/peningkatan kesadaran (*Awareness)* bagi seluruh *stakeholder* TIK.

b) Peningkatan pengetahuan/ketrampilan melalui program pelatihan dalam kelas, *on the job, online* dan kombinasinya. Program pelatihan dimaksud terdiri dari antara lain :

(1) *Information Security and Risk Management.*

(2) *Access Control Systems and Methodology.*

(3) *Cryptography.*

(4) *Physical Security.*

(5) *Telecommunications and Network Security.*

(6) *Security Architecture and Models.*

(7) *Business Continuity Planning and Disaster Recovery Plan.*

(8) *Applications Security.*

(9) *Operations Security.*

(10) *Legal, Regulations, Compliance and Investigations.*

(11) Implementasi SNI 27001.

c) Pengetahuan dan ketrampilan penanganan Insiden yang harus dimiliki meliputi sekurang-kurangnya dibidang :

(1) Pengetahuan *Digital Forensic.*

(2) Pengetahuan *Incident Response.*

(3) Pengetahuan sistem operasi.

(4) Pengetahuan tentang jaringan komunikasi data.

d) Pengetahuan dan ketrampilan untuk melakukan uji penetrasi (*Penetration Test)* yang dibutuhkan adalah sekurang-kurangnya :

(1) Pengetahuan dan ketrampilan keamanan informasi secara umum.

(2) Pengetahuan dan ketrampilan menggunakan alat-alat bantu *penetration testing*.

(3) Pengetahuan dan ketrampilan pengujian TI dan pelaporan.

(4) Pengetahuan dan ketrampilan pengembangan aplikasi berbasis *web/online.*

e) Pengetahuan dan ketrampilan uji kesesuaian (*System Assurance*).

f) Pengetahuan dan ketrampilan sistem yang meliputi :

(1) *Network Security (TCP/IP, LAN/WLAN, Routing: Static & RIP, Sniffing, Firewall).*

(2) *Operating Systems Security (Windows, Linux, Virtualization).*

(3) *Systems Infrastructure and Database Security (DHCP, DNS, RADIUS, OTP, CA, LDAP, FTP, Email, Web, MySQL).*

(4) *Digital Control System.*

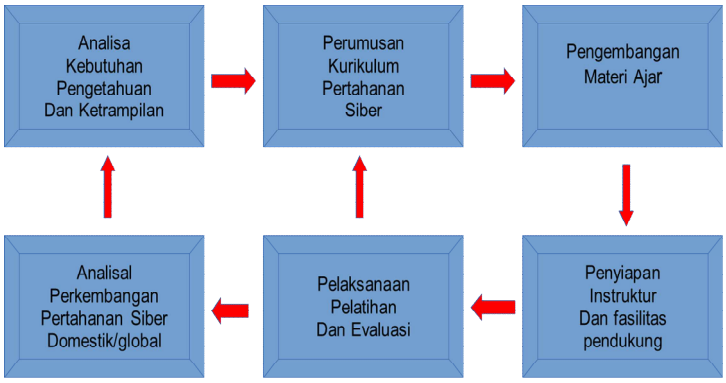
(5) *System Development* .

g) Pengetahuan dan kemampuan untuk merehabilitasi dan rekonstruksi kerusakan-kerusakan yang terjadi pada jaringan TIK dan muatannya.

h) Kurikulum bagi pendidikan dan latihan tersebut secara

berkala harus ditinjau ulang kesesuaiannya dengan kompetensi SDM Pertahanan Siber, mengingat cepatnya perkembangan teknologi dan dinamisnya peta kondisi keamanan siber global. Pengembangan kurikulum dan materi ajar yang diberikan harus disesuaikan dengan profil pembelajaran yang dapat berbeda-beda sesuai dengan instansi yang terlibat dalam Pertahanan Siber. Selengkapnya penyusunan kurikulum dan materi ajar perlu mengacu pada kerangka kerja yang terdapat pada bagan di bawah ini :

.



4.3. Tahapan Penyelenggaraan Pertahanan Siber

a. Tahap Pencegahan Serangan

1) Menerapkan arsitektur pengamanan informasi tingkat tinggi.

2) Membuat, mengimplementasikan dan mengoperasikan secara efektif arsitektur yang mencakup seluruh tahap siklus pertahanan siber agar mampu mengatasi ancaman terhadap faktor orang, logikal dan teknologi dari penyerang yang memiliki sumber daya yang besar dan akses yang luas dari berbagai aspek antara lain keuangan, teknologi, intelijen dan politik.

3) Kebijakan dan Prosedur pengamanan informasi tingkat tinggi.

4) Kebijakan dan prosedur pengamanan yang mengintegrasikan faktor pengamanan SDM, logikal dan fisik agar mampu mengatasi berbagai ancaman tingkat tinggi secara efektif.

5) Pengamanan SDM tingkat tinggi.

6) Memiliki personel yang berintegritas tinggi dan profesional untuk membangun dan mengimplementasikan arsitektur pengamanan informasi serta mengoperasikannya secara efektif.

7) Pengamanan logikal tingkat tinggi, yang berlapis dan terstruktur, serta terintegrasi dengan faktor pengamanan SDM dan fisik.

8) Pengamanan fisik tingkat tinggi, yang berlapis dan terstruktur, serta terintegrasi dengan faktor keamanan orang dan keamanan fisik.

b. Tahap Pemantauan Pengamanan Informasi

1) Pengawasan yang aman melakukan pengawasan logikal dan fisik yang berintegritas dan berkerahasiaan tinggi serta mampu mendeteksi setiap proses yang tidak terotorisasi.

2) Analisa Kelemahan yang aman. Menganalisa manajemen pengamanan yang mampu menjaga kerahasiaan informasi.

3) Pengalih Serangan. Melakukan pengalihan serangan agar sistem utama terhindar dari ancaman dan dapat mempelajari teknik serangan yang dilakukan.

4) Peringatan yang aman. Memberikan peringatan *real time* berlapis agar dapat menjamin ketersediaan, kerahasiaan dan integritas dari peringatan yang diberikan.

c. Tahap Analisis Serangan

1) Analisa Peringatan Serangan. Menganalisa serangan dengan dukungan implementasi yang efektif dari arsitektur pengamanan tingkat tinggi yang telah ditetapkan.

2) Analisa Piranti Lunak Berbahaya. Menganalisa secara mendalam piranti lunak berbahaya yang ditemukan.

3) Investigasi dan Forensik Digital. Melakukan proses investigasi dan forensik digital secara efektif sesuai dengan prosedur untuk memastikan integritas hasil dari proses yang dilakukan.

d. Tahap Pertahanan

1) Isolasi Serangan. Mengisolasi serangan dengan dukungan implementasi yang efektif dari arsitektur pengamanan tingkat tinggi yang telah ditetapkan, guna mengurangi dampak yang ditimbulkan.

2) Pencarian *Malware*. Menemukan *backdoor*, *trojan* dan *malware* lainnya agar tidak menjadi potensi ancaman dikemudian hari.

3) Perbaikan Sistem dan Data. Memperbaiki sistem dan data yang telah diserang.

4) Pemulihan Bencana. Melakukan pemulihan sistem dan data ketika terjadi bencana.

5) Pertimbangan Hukum dan Diplomatik. Melakukan pertimbangan hukum dan diplomatik untuk menentukan langkah-langkah selanjutnya, termasuk untuk melaporkan ke otoritas hukum dan memilih opsi serangan balik atau tidak.

6) Koordinasi Dengan Organisasi Terkait. Melakukan koordinasi penanganan serangan dengan organisasi-organisasi terkait.

e. Tahap Serangan Balik. Serangan balik merupakan suatu pilihan yang harus dipertimbangkan secara matang baik dari sisi hukum dan diplomasi. Beberapa contoh serangan balik yang dapat dilakukan oleh tim khusus, antara lain peretasan, penanaman *malware*, perusakan sistem dan rekayasa kondisi.

f. Tahap Peningkatan Pengamanan Informasi. Peningkatan pengamanan informasi harus selalu dilakukan berdasarkan hasil-hasil pada tahapan-tahapan sebelumnya. Peningkatan pengamanan dapat dilakukan pada salah satu atau keseluruhan dari faktor-faktor arsitektur pengamanan informasi meliputi pengamanan SDM, pengamanan logikal dan pengamanan fisik.

Tatacara lebih rinci dari implementasi masing-masing tahapan penyelenggaraan pertahanan siber seperti di atas, akan dibuat oleh satker pelaksana di bidang pertahanan siber. Tahapan tersebut di atas digambarkan dalam siklus pertahanan siber yang terdapat pada lampiran III.

4.4. Pentahapan Kegiatan Pertahanan Siber

Dalam mendukung aspek-aspek persiapan, pengembangan dan pengoperasian pertahanan siber sebagaimana diuraikan di atas, perlu disediakan anggaran yang terprogram agar kebutuhan tersebut dapat terpenuhi secara lengkap dan tepat waktu. Selanjutnya pentahapan operasional Pertahanan Siber Kemhan/TNI dilaksanakan sebagai berikut :

a. Tahap Persiapan

Dalam tahapan ini dilaksanakan dua fokus kegiatan yaitu :

1) Tim Kerja (*Desk*) Pertahanan Siber Kementerian Pertahanan, melaksanakan penyusunan produk kebijakan Pertahanan Siber, sebagai berikut :

a) Peta Jalan Strategi Nasional Pertahanan Siber.

b) Peta Jalan Pembinaan Kemampuan SDM Pertahanan Siber.

c) Rancangan Permenhan tentang Pusat Operasi Pertahanan Siber.

d) Rancangan Permenhan tentang pengamanan informasi di lingkungan Kemhan/TNI.

2) Pusdatin Kemhan melanjutkan kegiatan pembangunan teknologi dan infrastruktur (*Cyber Operation Center/COC*) pertahanan siber, sesuai dengan Standar Nasional Indonesia (SNI) 27001 tentang Sistem Manajemen Keamanan Informasi yang handal.

Output :

1) Produk Kebijakan yang dihasilkan Tim Kerja (*Desk*) Pertahanan Siber Kementerian Pertahanan, yaitu :

a) Peta Jalan Strategi Nasional Pertahanan Siber.

b) Peta Jalan Pembinaan Kemampuan SDM Pertahanan Siber.

c) Rancangan Permenhan tentang Pusat Operasi Pertahanan Siber.

d) Rancangan Permenhan tentang pengamanan informasi di lingkungan Kemhan/TNI.

2) Layanan sistem informasi dan keamanan infrastruktur TIK internal Kemhan/TNI sebagai langkah persiapan bagi manajemen informasi yang baik.

b. Tahap Pematangan

Pada tahap ini dilaksanakan fokus kegiatan Pertahanan Siber sebagai berikut :

1) Implementasi Penyelenggaraan Pertahanan Siber Kementerian Pertahanan dimulai dengan penetapan kelembagaan organisasi Pertahanan Siber.

2) Melaksanakan pengawasan audit sistem manajemen pengamanan informasi Kemhan/TNI secara independen dengan cakupan SDM, Proses dan Teknologi sesuai dengan SNI 27001 dan praktik terbaik pengamanan sistem informasi yang ditetapkan Kemkominfo (*ISSAF, OWASP, PCI-DSS*, dll) dalam melihat kesiapan pertahanan siber Kemhan/TNI.

3) Melaksanakan perekrutan dan pembinaan SDM Pertahanan Siber yang kompetitif berstandar nasional dan berskala internasional, peningkatan pelatihan pertahanan siber antara lain melalui kegiatan pelatihan, seminar, lokakarya pengamanan informasi di dalam dan luar negeri.

4) Menyiapkan *dashboard* sistem informasi infrastruktur yang tersambung dengan sistem infrastruktur Pertahanan Siber

lintas sektoral guna *updating* kebijakan dan strategi pertahanan siber.

5) Pengembangan ruang komando dan pengendalian sistem pertahanan siber (*Cyber Operation Center*) termasuk sistem sarana dan prasarana pelatihan dan penelitian, dengan mengacu kepada praktik terbaik (*best practises*) dan memperhatikan kemandirian dan kedaulatan.

6) Menyusun konsep dan implementasi kemandirian infrastruktur teknologi informasi dan komunikasi dalam rangka kedaulatan siber menggunakan satelit pertahanan secara mandiri, dengan kajian yang melibatkan berbagai pemangku kepentingan terkait.

7) Penyempurnaan dan peningkatan *Grand Design* Arsitektur *Enterprise* Sisfohanneg dan sistem informasi Pertahanan Siber yang selalu memperhatikan kemajuan teknologi dan kondisi sosial masyarakat.

8) Menyusun *IT Security Technology Policy* berbasis risiko bagi Pertahanan Siber untuk perangkat lunak maupun perangkat keras.

9) Melaksanakan kegiatan kerjasama operasional dengan kementerian / lembaga nasional.

Output :

1) Terlaksananya implementasi Penyelenggaraan Pertahanan Siber Kementerian Pertahanan, yang dimulai dengan penetapan kelembagaan organisasi Pertahanan Siber.

2) Terlaksananya pengawasan audit sistem manajemen pengamanan informasi Kemhan/TNI secara independen dengan cakupan SDM, Proses dan Teknologi sesuai dengan SNI 27001 dan praktik terbaik pengamanan sistem informasi yang ditetapkan Kemkominfo (*ISSAF, OWASP, PCI-DSS*, dll) dalam melihat kesiapan pertahanan siber Kemhan/TNI.

3) Terlaksananya perekrutan dan pembinaan SDM Pertahanan Siber yang kompetitif berstandar nasional dan berskala internasional, peningkatan pelatihan pertahanan siber antara lain melalui kegiatan pelatihan, seminar, lokakarya pengamanan informasi di dalam dan luar negeri.

4) Tersedianya *dashboard* sistem informasi infrastruktur yang tersambung dengan sistem infrastruktur Pertahanan Siber lintas sektoral guna *updating* kebijakan dan strategi pertahanan siber.

5) Terwujudnya pengembangan ruang komando dan pengendalian sistem pertahanan siber *(Cyber Operation Center*) termasuk sistem sarana dan prasarana pelatihan dan penelitian, dengan mengacu kepada praktik terbaik (*best practises*) dan memperhatikan kemandirian dan kedaulatan.

6) Terwujudnya konsep dan implementasi kemandirian infrastruktur teknologi informasi dan komunikasi dalam rangka kedaulatan sibe menggunakan satelit pertahanan secara mandiri, dengan kajian yang melibatkan berbagai pemangku kepentingan terkait.

7) Terwujudnya penyempurnaan dan peningkatan *Grand Design* Arsitektur *Enterprise* Sisfohanneg dan sistem informasi Pertahanan Siber yang selalu memperhatikan kemajuan teknologi dan kondisi sosial masyarakat.

8) Tersusunnya *IT Security Technology Policy* berbasis risiko bagi Pertahanan Siber untuk perangkat lunak maupun perangkat keras.

9) Terlaksananya kegiatan kerjasama operasional dengan kementerian / lembaga nasional.

c. Tahap Pemanfaatan

Pada tahap ini diharapkan akan dihasilkan kemampuan daya tangkal, daya tindak dan daya pulih dalam menghadapi serangan siber. Adapun kegiatan yang akan dilaksanakan dalam tahap ini adalah :

1) Implementasi sertifikasi standar terbaik pengamanan informasi berbasis SNI/ISO 27001.

2) Kelanjutan pembenahan pertahanan siber internal Kemhan/TNI berdasarkan hasil audit pengamanan TIK di tahap sebelumnya.

3) Pengembangan Infrastruktur teknologi Informasi dan komunikasi, melalui kegiatan riset dan pengembangan yang melibatkan lembaga profesional dibidang siber.

4) Pengembangan kemampuan profesional SDM TIK bersertifikasi sesuai dengan standar yang ditetapkan Pemerintah.

5) Pengembangan Sistem Informasi Pertahanan Siber.

6) Pengembangan kerja sama operasional lintas sektoral dan fasilitas strategis nasional.

7) Peningkatan kemampuan pertahanan siber yang optimal.

8) Kerja sama internasional sistem pertahanan siber.

Output :

1) Terlaksananya implementasi sertifikasi standar terbaik pengamanan informasi berbasis SNI/ISO 27001.
2) Terlaksananya kelanjutan pembenahan pertahanan siber internal Kemhan/TNI berdasarkan hasil audit pengamanan TIK di tahap sebelumnya.
3) Terwujudnya pengembangan Infrastruktur teknologi Informasi dan komunikasi, melalui kegiatan riset dan pengembangan yang melibatkan lembaga profesional dibidang siber.
4) Tercapainya peningkatan pengembangan kemampuan profesional SDM TIK bersertifikasi sesuai dengan standar yang ditetapkan Pemerintah.
5) Tercapainya peningkatan pengembangan Sistem Informasi Pertahanan Siber.
6) Terlaksananya kerja sama operasional lintas sektoral dan fasilitas strategis nasional.
7) Tercapainya peningkatan kemampuan pertahanan siber yang optimal.
8) Terwujudnya kerja sama internasional sistem pertahanan siber.

d. Tahap Optimalisasi

Fokus dalam tahap ini adalah memastikan kesiapan kemampuan (*capability*) dalam pertahanan siber yang lebih maju dalam segala pengertiannya, yang diharapkan sudah harus siap pada tahap ini. Kegiatan yang dilakukan pada tahun ini adalah :

1) Melaksanakan uji coba pertahanan siber terhadap serangan yang berskala luar biasa (*massive)* dengan instansi lain, dalam melihat kesiapan *CSIRT (Computer Security Insident Response Team*) dan sosialisasi pengamanan informasi berdasarkan hasil kegiatan di atas.
2) Melanjutkan kegiatan riset dan pengembangan dalam hal pertahanan siber.
3) Pengembangan pertahanan dan optimalisasi sistem TIK Kemhan/TNI.
4) Melakukan pengembangan pelatihan pertahanan siber dan mengikuti kompetisi pertahanan siber di lokal dan internasional.

5) Melakukan asesmen risiko keamanan sistem TIK oleh pihak independen dengan lingkup SDM, Proses dan Teknologi terhadap aset TIK di Kemhan/TNI.

6) *Maintenance* sertifikasi terhadap standard praktik terbaik pengamanan informasi berbasis SNI 27001.

Output :

1) Terlaksananya uji coba pertahanan siber terhadap serangan yang berskala luar biasa (*massive*) dengan instansi lain, dalam melihat kesiapan *CSIRT* (*Computer Security Insident Response Team*) dan sosialisasi pengamanan informasi berdasarkan hasil kegiatan di atas.

2) Berlanjutnya kegiatan riset dan pengembangan dalam hal pertahanan siber.

3) Terwujudnya pengembangan pertahanan dan optimalisasi sistem TIK Kemhan/TNI.

4) Terlaksananya pengembangan pelatihan pertahanan siber dan mengikuti kompetisi pertahanan siber di lokal dan internasional.

5) Terlaksananya asesmen risiko pengamanan sistem TIK oleh pihak independen dengan lingkup SDM, Proses dan Teknologi terhadap asset TIK di Kemhan/TNI.

6) Terlaksananya *maintenance* sertifikasi terhadap standard praktik terbaik pengamanan informasi berbasis SNI 27001.

BAB V

PENUTUP

Pedoman Pertahanan siber merupakan acuan penyelenggaraan kegiatan pertahanan siber yang harus dipahami, dipedomani dan dilaksanakan oleh seluruh satuan kerja Kemhan/TNI, sesuai dengan tugas pokok dan fungsinya masing-masing.

Jakarta, 2014

Menteri Pertahanan,

Purnomo Yusgiantoro

DAFTAR PUSTAKA

Boisot, M. (1998). *Knowledge Assets. Oxford : Oxford University Press*.

Carr, J. (2009). *Inside Cyber Warfare : Mapping the Cyber Underworld. O'Reilly Media*.

Clarke, R. A., & Knake, R. K. (2010). *Cyber War.* New York : Harper Colins.

Erbschloe, M. (2001). *Information Warfare : How to Survive Cyber Attacks.* New York : *The McGraw-Hill*.

Ghernaouti, S. (2009). C*ybersecurity Guide for Developing Countries.* Geneva : *International Telecommunication Union*.

Graham, J., Olson, R., & Howard, R. (2009). *Cyber Security Essential. Auerbach Publications*.

Hutchinson, B., & Warren, M. (2001). *Information Warfare.* Oxford : Butterworth-Heinemann.

Kementerian Pertahanan RI. (2008). Doktrin Pertahanan Negara. Jakarta : Kementerian Pertahanan.

Kementerian Komunikasi dan Informatika RI. (2010). Buku Putih Kominfo. Jakarta: Kemkominfo.

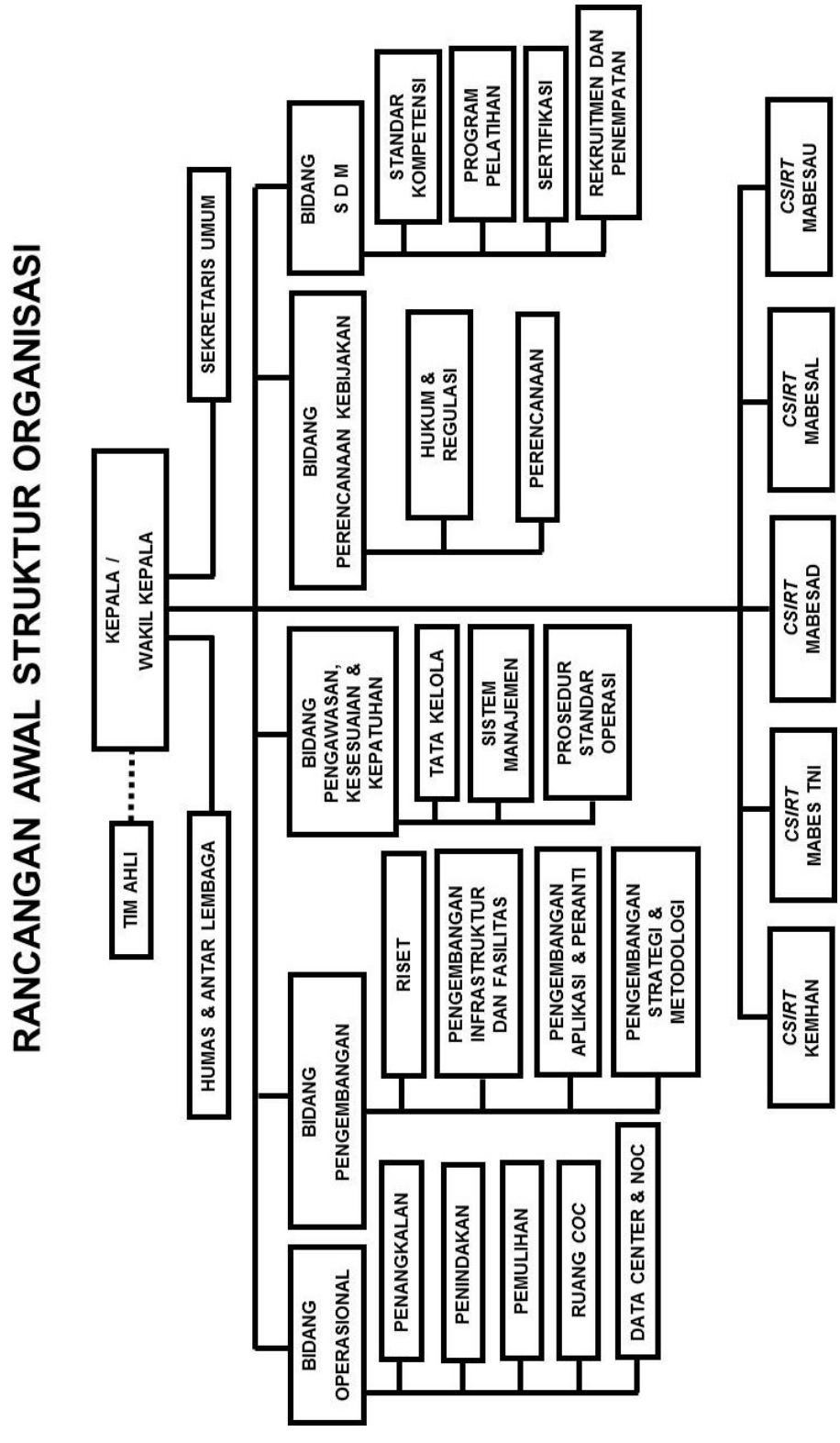
Shoemaker, D., & Conklin, A. (2011). *Cyber Security : The Essentials Body of Knowledge. Delmar Cengage Learning*.

Wamala, F. (2011). *The ITU National Cyber Security Strategy Guide.* Geneva : *International Telecommunication Union.*

LAMPIRAN I

RANCANGAN AWAL STRUKTUR ORGANISASI

RANCANGAN AWAL STRUKTUR ORGANISASI



LAMPIRAN II

RANCANGAN UMUM SPESIFIKASI TEKNIS
TEKNOLOGI DAN INFRASTRUKTUR
PERTAHANAN SIBER

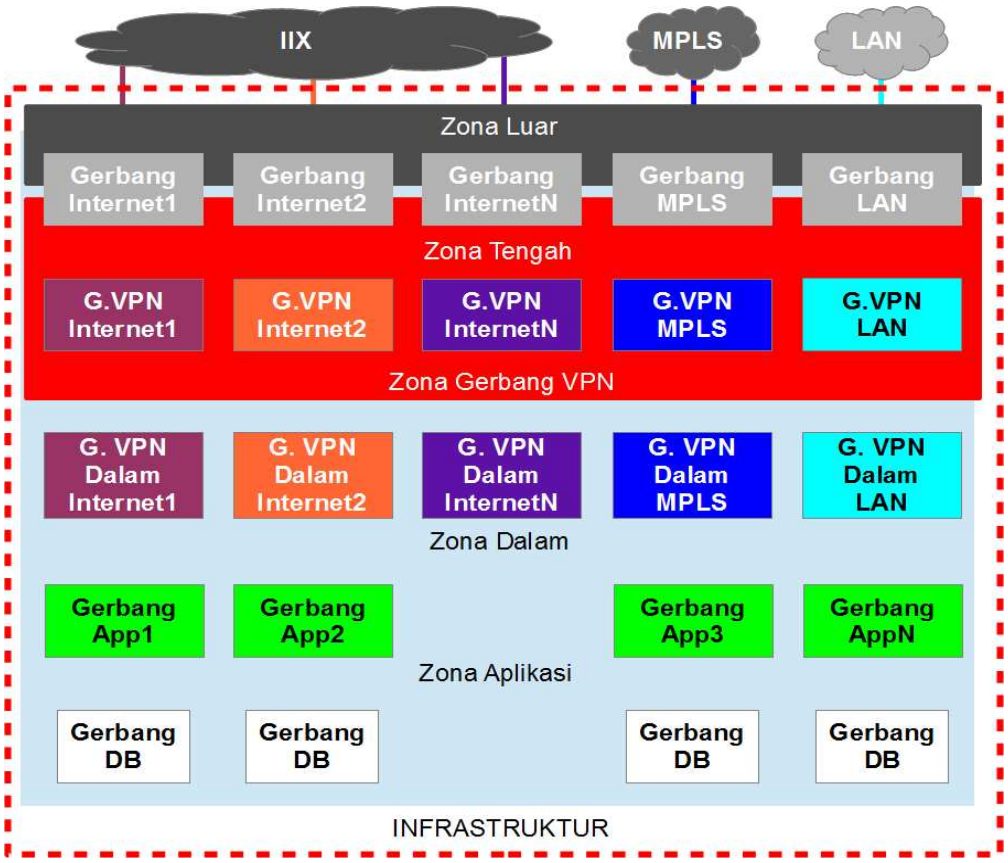
RANCANGAN UMUM SPESIFIKASI TEKNIS TEKNOLOGI DAN INFRASTRUKTUR PERTAHANAN SIBER

1. Rancangan umum teknologi dan infrastruktur Pertahanan Siber sekurang-kurangnya memenuhi arsitektur sebagai berikut :
   a. Rancangan Global Pengamanan Infrastruktur
      1) Dasar-Dasar Perancangan
         a) Alokasi gerbang akses berdasarkan fungsi dan jenis koneksi.
         b) Rancangan pola alur akses yang aman.
         c) Konsep alur akses informasi yang aman.
         d) Konsep alur akses administrasi sistem yang aman.
         e) Peta koneksi logikal jaringan.
         f) Rancangan arsitektur *routing* area.
         g) Peta implementasi komponen pengamanan TI.
         h) Rancangan arsitektur global pengamanan TI.
      2) Zona Aplikasi. Setiap Aplikasi memiliki beberapa zona yang terdiri dari :
         a) Zona Produksi Data *Input.*
         b) Zona Produksi Data *Output.*
         c) Zona Uji Coba.
         d) Zona Pengembangan.
      3) Pengamanan berlapis
         a) Menggunakan beberapa jenis produk pengamanan informasi.
         b) Setiap segmen jaringan harus dibatasi dengan i yang berbeda.
         c) Setiap koneksi fisik harus diamankan menggunakan enkripsi jaringan (*VPN*).
         d) Memungkinkan integrasi algoritma enkripsi privat untuk jaringan dan media penyimpan.
         e) Memungkinkan penggunaan 2 atau lebih algoritma enkripsi berbeda untuk jaringan dan media penyimpan.
      4) Pengawasan berlapis
         a) Sistem deteksi intrusi di setiap segmen jaringan.

b) Sistem pengawasan integritas sistem operasi dan aplikasi.

c) Sistem pengawasan aktivitas pengguna dan *administrator*.

b. Rancangan Pengamanan Jaringan



1)

Gerbang, terdiri dari:

a) Gerbang Luar.

b) Gerbang *VPN* Luar.

c) Gerbang *VPN* Dalam.

d) Gerbang Aplikasi.

e) Gerbang *Database*.

2) Sistem Deteksi Intrusi (SDI) Jaringan, terdiri dari :

a) SDI Luar untuk mengawasi Zona Luar, Zona Tengah, Zona Gerbang VPN.

b) SDI Dalam untuk mengawasi Zona Dalam.

c) SDI *Core* dan Aplikasi untuk mengawasi Zona Inti, Zona Akses Aplikasi, Zona *Database*.

c. Rancangan Keamanan *Server*

1) Sistem Penjaminan Integritas.

2) Enkripsi *Disk.*

d. Rancangan Keamanan Aplikasi

1) *Source Code Library.*

2) Source Code Analyzer.

e. Rancangan Keamanan Klien

1) Enkripsi keseluruhan media penyimpan dengan manajemen kunci yang aman.

2) Enkripsi aplikasi, seperti *email*, *instant messaging*, *SMS*, suara, dan aplikasi *web* dengan manajemen kunci yang aman.

3) Hanya dapat berkomunikasi ke spesifik alamat *IP* gerbang *VPN.*

4) Untuk informasi dengan tingkat keamanan maksimum, brankas digital milik pengguna hanya dapat dibuka dengan menggunakan kunci yang dimiliki pengguna dan kunci yang dimiliki infrastruktur.

f. Rancangan Keamanan *Backup*

1) Enkripsi media penyimpan dengan manajemen kunci yang aman.

2) Brankas tahan api untuk mengamankan media penyimpan.

g. Rancangan Keamanan Penghancuran Data

Memastikan penghancuran informasi digital dan fisik agar tidak dapat dipulihkan kembali.

2. Rancangan khusus teknologi dan infrastruktur Pertahanan Siber sekurang-kurangnya memenuhi arsitektur sebagai berikut :

a. Infrastruktur Aplikasi

1) Infrastruktur Aplikasi Umum.

a) *Secure Content Management System.*

b) *Secure File Transfer.*

c) *Secure Email.*

d) *Secure Instant Messaging.*

e) *Secure Voice.*

f) *Secure Teleconference.*

g) *Secure Ticketing.*

h) *Secure Printing.*

2) Infrastruktur Aplikasi *E-Govt* (didefinisikan sesuai kebutuhan).

3) Infrastruktur Aplikasi Manajemen Pengamanan.

a) *Secure Patch Management.*

b) Secure Access Authorization Management.

c) Secure Change Management.

d) Secure Inventory Management.

4) Infrastruktur Aplikasi Pengamanan Logikal.

a) Pencegahan.

(1) Infrastruktur Dasar TI.

(a) *Secure External DNS.*

(b) *Secure Internal DNS.*

(c) *Secure DHCP.*

(d) *Secure Time Reference.*

(2) Infrastruktur Keamanan TI.

(a) Infrastruktur Kunci Publik.

(b) Otentikasi Kuat.

(c) Manajemen Kunci Enkripsi.

(3) Infrastruktur Pengamanan Fisik.

(a) *Secure Access Control System.*

(b) *Secure Smart Surveillance System.*

(4) Infrastruktur Administrasi Sistem.

Secure Administrator Virtual Desktop.

(5) Infrastruktur Pengguna.

Secure User Virtual Desktop.

(6) Infrastruktur Administrasi Kode Sumber.

Secure Application Library and Escrow.

b) Pemantauan.

(1) Infrastruktur *Centralized Log.*

(2) Infrastruktur Penjaminan Integritas.

(3) Infrastruktur *Real Time Monitoring.*

(a) *SIEM.*

(b) *Secure Real Time Alert.*

(4) Infrastruktur Pengujian Keamanan.

(5) Infrastruktur Pengalih Serangan.

c) Analisa.

(1) Infrastruktur *Attack Analysis.*

(2) Infrastruktur *Malware Analysis.*

(3) Infrastruktur *Digital Forensic.*

d) Pertahanan.

(1) Infrastruktur Pengelolaan Insiden.

(2) Serangan (Opsional).

b. Infrastruktur Pengamanan Fisik.

1) Ruang Pusat Operasi Utama.

2) Memiliki pusat data berkwalifikasi *Tier-2*.

3) Memiliki fungsi *Tempest*.

4) Proses otentikasi dan otorisasi akses memiliki keamanan tingkat tinggi.

5) Diawasi 24x7 melalui *CCTV* oleh pengamanan SDM.

6) Dijaga 24x7 oleh pengamanan SDM.

a) Ruang Pusat Operasi Darurat.

(1) Memiliki fasilitas *rack server* berkunci elektronik dan fisik, pendinginan dan kelistrikan berkwalifikasi *Tier*-1.

(2) Memiliki fungsi *Tempest.*

(3) Proses otentikasi dan otorisasi akses memiliki keamanan tingkat tinggi.

(4) Diawasi 24x7 oleh pengamanan SDM melalui *CCTV*.

(5) Dijaga 24x7 oleh pengamanan SDM.

b) Pusat Data Utama.

(1) Pusat data berkwalifikasi *Tier*-3.

(2) Memiliki fungsi *Tempest*.

(3) Proses otentikasi dan otorisasi akses memiliki

keamanan tingkat tinggi.

(4) Diawasi 24x7 oleh pengamanan SDM melalui *CCTV*.

(5) Dijaga 24x7 oleh pengamanan SDM.

c) Pusat Data Cadangan.

(1) Pusat data berkwalifikasi *Tier*-3.

(2) Memiliki fungsi *Tempest*.

(3) Proses otentikasi dan otorisasi akses memiliki keamanan tingkat tinggi.

(4) Diawasi 24x7 oleh pengamanan SDM melalui *CCTV*.

(5) Dijaga 24x7 oleh pengamanan SDM.

d) Ruang Perangkat *Server* dan Jaringan.

(1) Memiliki fasilitas *rack server* berkunci elektronik dan fisik, pendinginan, pemadam api dan kelistrikan berkwalifikasi *Tier*-1.

(2) Memiliki fungsi *Tempest*.

(3) Proses otentikasi dan otorisasi akses memiliki keamanan tingkat tinggi.

(4) Diawasi 24x7 oleh pengamanan SDM melalui *CCTV*.

e) Ruang Kerja Pengguna untuk memproses informasi dengan tingkat keamanan maksimum :

(1) Memiliki fungsi *Tempest*.

(2) Proses otentikasi dan otorisasi akses memiliki keamanan tingkat tinggi.

(3) Diawasi 24x7 oleh pengamanan SDM melalui *CCTV*.

f) Ruang Pencetakan untuk memproses informasi dengan tingkat keamanan maksimum :

(1) Memiliki fungsi *Tempest*.

(2) Proses otentikasi dan otorisasi akses memiliki keamanan tingkat tinggi.

(3) Diawasi 24x7 oleh pengamanan SDM melalui *CCTV*.

LAMPIRAN III

SIKLUS PERTAHANAN SIBER

SIKLUS PERTAHANAN SIBER