KEMENTERIAN PERTAHANAN REPUBLIK INDONESIA
BADAN INSTALASI STRATEGIS PERTAHANAN

PERATURAN KEPALA BADAN INSTALASI STRATEGIS PERTAHANAN KEMENTERIAN PERTAHANAN NOMOR 03 TAHUN 2022

TENTANG

MEKANISME PENETAPAN ANCAMAN SIBER TERHADAP PENYELENGGARAAN PERTAHANAN NEGARA DI LINGKUNGAN KEMENTERIAN PERTAHANAN

DITETAPKAN DI JAKARTA
PADA TANGGAL 30 DESEMBER 2022

KEMENTERIAN PERTAHANAN REPUBLIK INDONESIA
BADAN INSTALASI STRATEGIS PERTAHANAN

PERATURAN KEPALA BADAN INSTALASI STRATEGIS PERTAHANAN
KEMENTERIAN PERTAHANAN
NOMOR 03 TAHUN 2022
TENTANG
MEKANISME PENETAPAN ANCAMAN SIBER
TERHADAP PENYELENGGARAAN PERTAHANAN NEGARA
DI LINGKUNGAN KEMENTERIAN PERTAHANAN

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN INSTALASI STRATEGIS PERTAHANAN
KEMENTERIAN PERTAHANAN,

Menimbang :

a. bahwa dalam menentukan cara tindak yang tepat terhadap ancaman siber yang mengganggu pertahanan negara atas pesatnya perkembangan teknologi pada saat ini, dari jenis, bentuk dan metodenya perlu dilakukan penetapan ancaman siber;
b. bahwa untuk menindaklanjuti hasil pengidentifikasian dan penilaian ancaman siber perlu adanya penetapan level risiko ancaman siber;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Kepala Badan Instalasi Strategis Pertahanan Kementerian Pertahanan tentang Mekanisme Penetapan Ancaman Siber Terhadap Penyelenggaraan Pertahanan Negara di lingkungan Kementerian Pertahanan;

Mengingat :

1. Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber (Berita Negara Republik Indonesia Tahun 2014 Nomor 1712);
2. Peraturan Menteri Pertahanan Nomor 14 Tahun 2019 tentang Organisasi dan Tata Kerja Kementerian Pertahanan (Berita Negara Republik Indonesia Tahun 2019 Nomor 314);
3. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber (Berita Negara Republik Indonesia Tahun 2020 Nomor 1488);

MEMUTUSKAN:

Menetapkan : PERATURAN KEPALA BADAN INSTALASI STRATEGIS PERTAHANAN KEMENTERIAN PERTAHANAN TENTANG MEKANISME PENETAPAN ANCAMAN SIBER TERHADAP PENYELENGGARAAN PERTAHANAN NEGARA DI LINGKUNGAN KEMENTERIAN PERTAHANAN.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Kepala Badan ini yang dimaksud dengan:

1. Penetapan adalah proses, cara, perbuatan menetapkan.
2. Ancaman Siber adalah segala upaya, kegiatan, dan/atau tindakan, baik dari dalam negeri maupun luar negeri, yang dinilai dan/atau dibuktikan dapat melemahkan, merugikan dan/atau menghancurkan infrastruktur informasi vital, sistem elektronik, data dan informasi Kementerian Pertahanan.
3. Insiden Siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya sistem elektronik.
4. Serangan Siber adalah Ancaman Siber yang mengakibatkan objek pengamanan siber menjadi tidak berfungsi, sebagian atau seluruhnya, dan/atau bersifat sementara atau permanen.
5. Kementerian Pertahanan yang selanjutnya disebut Kemhan adalah kementerian yang menyelenggarakan urusan pemerintahan di bidang pertahanan.
6. Menteri adalah menteri yang menyelenggarakan urusan pemerintahan di bidang pertahanan.
7. Badan Instalasi Strategis Pertahanan Kemhan yang selanjutnya disebut Bainstrahan Kemhan adalah badan yang mempunyai tugas melaksanakan pengelolaan instalasi strategis, pertahanan siber dan informasi pertahanan.
8. Kepala Bainstrahan Kemhan yang selanjutnya disebut Kabainstrahan Kemhan adalah kepala badan yang mempunyai tugas melaksanakan pengelolaan instalasi strategis, pertahanan siber dan informasi pertahanan.
9. Pusat Pertahanan Siber yang selanjutnya disebut Pushansiber adalah unsur pelaksana tugas dan fungsi Bainstrahan Kemhan.
10. Kepala Pushansiber yang selanjutnya disebut Kapushansiber adalah kepala pusat yang melaksanakan tugas dan fungsi Bainstrahan Kemhan di bidang tata kelola, kerja sama, operasi, dan jaminan keamanan pertahanan siber.

Pasal 2

Peraturan Kepala Badan ini disusun dengan maksud sebagai pedoman dalam mekanisme Penetapan Ancaman Siber terhadap penyelenggaraan pertahanan Negara di lingkungan Kemhan.

Pasal 3

(1) Penetapan Ancaman Siber bertujuan untuk mengesahkan level risiko Ancaman Siber.
(2) Pengesahan level risiko Ancaman Siber meliputi level risiko tinggi, level risiko sedang dan level risiko rendah.

Pasal 4

Level risiko sebagaimana dimaksud dalam Pasal 3 ayat (2) merupakan pedoman di dalam menentukan prioritas penanganan Ancaman Siber.

Pasal 5

Manfaat Penetapan Ancaman Siber untuk:
a. merealisasikan kebijakan yang cepat;
b. kejelasan dalam cara penanganan Ancaman Siber; dan
c. mengatasi dampak kerusakan akibat Ancaman Siber.

BAB II
PENETAPAN ANCAMAN SIBER

Bagian Kesatu
Penetapan

Pasal 6

Penetapan Ancaman Siber memiliki fungsi untuk mengesahkan:
a. jenis Ancaman Siber;
b. bentuk Ancaman Siber;
c. metode Ancaman Siber; dan
d. risiko Ancaman Siber.

Paragraf 1
Jenis Ancaman Siber

Pasal 7

(1) Jenis Ancaman Siber sebagaimana dimaksud dalam Pasal 6 huruf a terdiri atas:
    a. ancaman perangkat keras (*hardware threat*);
    b. ancaman perangkat lunak (*software threat*);
    c. ancaman data/informasi (data/*information threat*); dan
    d. jenis Ancaman Siber lainnya.
(2) Ancaman perangkat keras (*hardware threat*) sebagaimana dimaksud pada ayat (1) huruf a merupakan ancaman yang disebabkan oleh pemasangan peralatan tertentu yang berfungsi untuk melakukan kegiatan tertentu dalam suatu sistem, sehingga peralatan tersebut menjadi gangguan terhadap sistem jaringan dan perangkat keras lainnya.
(3) Ancaman perangkat lunak (*software threat*) sebagaimana dimaksud pada ayat (1) huruf b merupakan 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*), ke dalam suatu sistem.

(4) Ancaman data/informasi (data/*information threat*) sebagaimana dimaksud pada ayat (1) huruf c merupakan ancaman yang diakibatkan oleh penyebaran data/informasi tertentu yang bertujuan untuk kepentingan tertentu, seperti yang dilakukan dalam information *warfare* termasuk kegiatan propaganda.

(5) Jenis Ancaman Siber lainnya sebagaimana dimaksud pada ayat (1) huruf d merupakan jenis Ancaman Siber yang belum terdeteksi dan/atau belum ada yang disebabkan oleh kemajuan teknologi informasi dan sistem elektronik.

Paragraf 2
Bentuk Ancaman Siber

Pasal 8

(1) Bentuk Ancaman Siber sebagaimana dimaksud dalam Pasal 6 huruf b terdiri atas:
   a. serangan *advanced persistent threats*;
   b. serangan berbasis *web*;
   c. penyusupan siber;
   d. *cyberspionage*; dan
   e. bentuk Ancaman Siber lainnya.

(2) Serangan *advanced persistent threats* sebagaimana dimaksud pada ayat (1) huruf a merupakan Serangan Siber yang kompleks, memakai banyak komponen yang berbeda untuk menyerang perangkat.

(3) Serangan berbasis *web* sebagaimana dimaksud pada ayat (1) huruf b menggunakan metode berbasis *web* atau skrip berbahaya yang mengarahkan korban ke situs *web* atau mengunduh konten berbahaya dan menyuntikkan kode berbahaya untuk mencuri data/informasi.

(4) Penyusupan siber sebagaimana dimaksud pada ayat (1) huruf c merupakan aktivitas ilegal yang dilakukan oleh peretas untuk masuk ke dalam sistem jaringan komputer korban melalui eksploitasi kerentanan yang ada pada sistem.

(5) *Cyberspionage* sebagaimana dimaksud pada ayat (1) huruf d merupakan tindakan pencurian informasi yang dilakukan oleh penyerang dengan tujuan untuk mengacaukan sistem politik, hak kekayaan intelektual, dan informasi kepemilikan di bidang strategis.

(6) Bentuk Ancaman Siber lainnya sebagaimana dimaksud pada ayat (1) huruf e merupakan bentuk Ancaman Siber yang belum terdeteksi dan/atau belum ada yang disebabkan oleh kemajuan teknologi informasi dan sistem elektronik.

Paragraf 3
Metode Ancaman Siber

Pasal 9

(1) Metode Ancaman Siber sebagaimana dimaksud dalam Pasal 6 huruf c terdiri atas:
   a. *denial of service* (dos) dan *distributed denial of service* (ddos);
   b. *defacement*;
   c. *phishing*;
   d. *malware;*
   e. *spam*;
   f. *spoofing*;
   g. *social engineering*;
   h. *insider threat*;
   i. *botnet*; dan
   j. metode Ancaman Siber lainnya.

(2) *Denial of service* (dos) dan *distributed denial of service* sebagaimana dimaksud pada ayat (1) huruf a jenis Serangan Siber yang dilakukan dengan melakukan *overloading* kapasitas sistem dan mencegah pengguna yang sah untuk mengakses dan menggunakan sistem atau sumber daya yang ditargetkan sehingga dapat mengganggu operasional sistem, dengan cara menghadapkan sistem pada permintaan akses dan proses yang jauh lebih besar dari yang bisa ditangani sistem.

(3) *Defacement* sebagaimana dimaksud pada ayat (1) huruf b merupakan metode Serangan Siber yang dilakukan dengan cara melakukan penggantian atau modifikasi terhadap halaman *website* korban sehingga isi dari halaman *website* korban berubah sesuai dengan motif penyerang.

(4) *Phishing* sebagaimana dimaksud pada ayat (1) huruf c merupakan metode Serangan Siber yang dilakukan dengan cara memberikan alamat *website* palsu dengan tampilan persis sama dengan *website* aslinya dengan tujuan untuk mendapatkan informasi penting dan sensitif milik korban.

(5) *Malware* sebagaimana dimaksud pada ayat (1) huruf d merupakan suatu program atau kode berbahaya yang dapat digunakan untuk mengganggu operasi normal dari sebuah sistem komputer.

(6) *Spam* sebagaimana dimaksud pada ayat (1) huruf e merupakan pengiriman surat elektronik yang dilakukan secara massal yang tidak dikehendaki oleh penerima dengan tujuan komersial atau publisitas, penyebaran *malware* ataupun mengganggu layanan surat elektronik milik penerima.

(7) *Spoofing* sebagaimana dimaksud pada ayat (1) huruf f merupakan serangan yang menargetkan protokol jaringan dengan tujuan untuk melewati sisi keamanan jaringan komputer.

(8) *Social engineering* sebagaimana dimaksud pada ayat (1) huruf g merupakan teknik manipulasi yang memanfaatkan kesalahan manusia untuk

mendapatkan akses pada informasi maupun data.

(9) *Insider threat* sebagaimana dimaksud pada ayat (1) huruf h merupakan ancaman terhadap keamanan atau data sebuah sistem yang berasal dari aktivitas orang yang sedang atau pernah bekerja dalam sebuah organisasi.

(10) *Botnet* sebagaimana dimaksud pada ayat (1) huruf i merupakan metode yang dilakukan penyerang untuk melakukan serangan yang beroperasi secara *peer-to-peer* atau dari pusat *command and control* dengan memanfaatkan jaringan perangkat yang saling terhubung dan terinfeksi oleh *malware bot.*

(11) Metode Ancaman Siber lainnya sebagaimana dimaksud pada ayat (1) huruf j merupakan metode Ancaman Siber yang belum terdeteksi dan/atau belum ada yang disebabkan oleh kemajuan teknologi informasi dan sistem elektronik.

Paragraf 4
Risiko Ancaman Siber

Pasal 10

(1) Risiko Ancaman Siber sebagaimana dimaksud dalam Pasal 6 huruf d terdiri dari level risiko dan prioritas risiko Ancaman Siber.

(2) Level risiko Ancaman Siber sebagaimana dimaksud pada ayat (1) terdiri dari level rendah, level sedang, dan level tinggi.

(3) Prioritas Ancaman Siber sebagaimana dimaksud pada ayat (1) merupakan variabel yang diutamakan dalam klasifikasi Ancaman Siber.

(4) Prioritas risiko Ancaman Siber sebagaimana dimaksud pada ayat (1) menentukan pengutamaan dalam cara tindak Ancaman Siber.

Bagian Kedua
Klasifikasi Ancaman Siber

Pasal 11

Klasifikasi Ancaman Siber terhadap penyelenggaraan pertahanan negara di lingkungan Kemhan dapat diklasifikasikan sebagai berikut:

a. ancaman yang dapat merusak dan/atau mengganggu infrastruktur informasi vital dan sistem elektronik pertahanan negara; dan

b. ancaman yang dapat merusak informasi elektronik dan data elektronik pertahanan negara.

Bagian Ketiga
Sumber dan Aspek Ancaman Siber

Pasal 12

Sumber Ancaman Siber merupakan entitas yang berkeinginan atau memiliki niat dan secara nyata akan melakukan kegiatan yang melanggar norma dan hukum, aturan dan ketentuan serta kaidah atau kontrol keamanan

informasi serta aset fisik lainnya.

Pasal 13

(1) Sumber ancaman sebagaimana dimaksud dalam Pasal 12 mempunyai tujuan untuk mendapatkan keuntungan yang bersifat materil dan *immateril.*
(2) Sumber ancaman sebagaimana dimaksud pada ayat (1) dapat diidentifikasi yang bersumber dari:
    a. internal dan eksternal;
    b. kegiatan intelijen;
    c. kekecewaan;
    d. investigasi;
    e. organisasi ekstremis;
    f. *hacktivists*;
    g. grup kejahatan terorganisir;
    h. persaingan, permusuhan, konflik; dan
    i. teknologi.

Pasal 14

(1) Aspek ancaman merupakan segala sesuatu yang melatarbelakangi terjadinya ancaman dan Serangan Siber.
(2) Aspek ancaman sebagaimana dimaksud pada ayat (1) meliputi 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.

Bagian Keempat
Dampak Serangan Siber

Pasal 15

Dampak yang mungkin dialami dari sebuah Serangan Siber berbentuk:
a. gangguan fungsional;
b. pengendalian sistem secara *remote*;
c. penyalahgunaan informasi;
d. kerusuhan, ketakutan, kekerasan, kekacauan, konflik; dan
e. kondisi lain yang sangat merugikan, sehingga memungkinkan dapat mengakibatkan kehancuran.

BAB III
MEKANISME PENETAPAN ANCAMAN SIBER

Pasal 16

(1) Mekanisme Penetapan Ancaman Siber dilaksanakan melalui rapat koordinasi dengan memperhatikan hasil identifikasi dan hasil penilaian.
(2) Rapat koordinasi sebagaimana dimaksud pada ayat (1) dipimpin oleh Kapushansiber Bainstrahan Kemhan dengan dihadiri oleh:
    a. Kepala Bidang Operasi Siber Pushansiber Bainstrahan Kemhan;
    b. Kepala Bidang Penjaminan Keamanan

Pushansiber Bainstrahan Kemhan;

c. Kepala Subbidang Pemantauan, Analisis dan Pelaporan Bidang Operasi Siber Pushansiber Bainstrahan Kemhan;
d. Kepala Subbidang Keamanan Aplikasi Bidang Penjaminan Keamanan Pushansiber Bainstrahan Kemhan;
e. Kepala Subbidang Keamanan Infrastruktur dan Komunikasi Bidang Penjaminan Keamanan Pushansiber Bainstrahan Kemhan;
f. Tim monitoring; dan
g. Tim penilai.

(3) Rapat koordinasi sebagaimana dimaksud pada ayat (2) untuk menghasilkan Penetapan Ancaman Siber.

Pasal 17

Penetapan Ancaman Siber sebagaimana dimaksud dalam Pasal 16 oleh Kapushansiber Bainstrahan Kemhan.

Pasal 18

Penetapan Ancaman Siber sebagaimana dimaksud dalam Pasal 17 sebagai dasar cara tindak terhadap Ancaman Siber.

BAB IV
PENGENDALIAN DAN PENGAWASAN

Pasal 19

Pengendalian mekanisme Penetapan Ancaman Siber terhadap penyelenggaraan pertahanan negara di lingkungan Kemhan dilaksanakan oleh Kabainstrahan Kemhan.

Pasal 20

Pengawasan mekanisme Penetapan Ancaman Siber terhadap penyelenggaraan pertahanan negara di lingkungan Kemhan dilaksanakan oleh Kapushansiber Bainstrahan Kemhan.

BAB V
KETENTUAN PENUTUP

Pasal 21

Peraturan Kepala Badan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 30 Desember 2022

KEPALA BADAN INSTALASI STRATEGIS PERTAHANAN
KEMENTERIAN PERTAHANAN,

YUDI ABRIMANTYO, S.I.P., M.Sc.
MAYOR JENDERAL TNI