KEMENTERIAN PERTAHANAN REPUBLIK INDONESIA
BADAN INSTALASI STRATEGIS PERTAHANAN

PERATURAN KEPALA BADAN INSTALASI STRATEGIS PERTAHANAN
KEMENTERIAN PERTAHANAN
NOMOR 01 TAHUN 2022

TENTANG

MEKANISME PENGIDENTIFIKASIAN 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 01 TAHUN 2022
TENTANG
MEKANISME PENGIDENTIFIKASIAN 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 untuk mengantisipasi dampak ancaman siber terhadap pertahanan negara atas pesatnya perkembangan teknologi pada saat ini, dari jenis, bentuk dan metodenya perlu dilakukan identifikasi penanganan pencegahan dan penanggulangan terhadap ancaman siber;
b. bahwa untuk menghadapi kemungkinan ancaman siber terhadap pertahanan negara perlu mekanisme pengidentifikasian ancaman siber agar lebih mudah mengetahui kemampuan dalam mendeteksi celah kerentanan dari infrastruktur informasi vital, sistem elektronik, informasi elektronik dan data elektronik;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Kepala Badan Instalasi Strategis Pertahanan Kementerian Pertahanan tentang Mekanisme Pengidentifikasian 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 PENGIDENTIFIKASIAN 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. Pengidentifikasian adalah proses atau cara dalam meneliti dan menelaah.
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. Serangan Siber adalah Ancaman Siber yang mengakibatkan objek pengamanan siber menjadi tidak berfungsi, sebagian atau seluruhnya, dan/atau bersifat sementara atau permanen.
4. Kementerian Pertahanan yang selanjutnya disebut Kemhan adalah kementerian yang menyelenggarakan urusan pemerintahan di bidang pertahanan.
5. Menteri adalah menteri yang menyelenggarakan urusan pemerintahan di bidang pertahanan.
6. Badan Instalasi Strategis Pertahanan Kemhan yang selanjutnya disebut Bainstrahan Kemhan adalah badan yang mempunyai tugas melaksanakan pengelolaan instalasi strategis, pertahanan siber dan informasi pertahanan.
7. Kepala Bainstrahan Kemhan yang selanjutnya disebut Kabainstrahan Kemhan adalah kepala badan yang mempunyai tugas melaksanakan pengelolaan instalasi strategis, pertahanan siber dan informasi pertahanan.
8. Pusat Pertahanan Siber yang selanjutnya disebut Pushansiber adalah unsur pelaksana tugas dan fungsi Bainstrahan Kemhan.
9. 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 Pengidentifikasian Ancaman Siber terhadap penyelenggaraan pertahanan negara di lingkungan Kemhan.

Pasal 3

Identifikasi Ancaman Siber bertujuan untuk mencari, mengetahui kemampuan dan mendeteksi celah kerentanan dari infrastruktur informasi vital, sistem elektronik, informasi elektronik dan data elektronik yang dimiliki dan digunakan di lingkungan Kemhan.

Pasal 4

Sasaran identifikasi Ancaman Siber meliputi seluruh infrastruktur informasi vital, sistem elektronik, informasi elektronik dan data elektronik yang dimiliki dan digunakan di lingkungan Kemhan.

Pasal 5

Objek identifikasi Ancaman Siber meliputi:

a. aset fisik dan perangkat lunak untuk menetapkan dasar program manajemen aset;
b. lingkungan kerja khususnya pada sektor infrastruktur informasi vital;
c. kebijakan dan/atau regulasi keamanan siber untuk menentukan tata kelola yang efektif dalam rangka menjamin sistem keamanan siber;
d. kerentanan aset, ancaman terhadap sumber daya internal dan eksternal dan aktivitas respons risiko sebagai dasar untuk penilaian risiko; dan
e. strategi manajemen risiko untuk menetapkan toleransi risiko.

BAB II

PENGIDENTIFIKASIAN ANCAMAN SIBER

Bagian Kesatu

Identifikasi

Pasal 6

Pengidentifikasian Ancaman Siber dilakukan dengan memperhatikan:

a. sistem elektronik dan data yang berpengaruh langsung terhadap kepentingan pertahanan negara; dan
b. sistem elektronik dan data yang tidak berpengaruh secara langsung terhadap kepentingan pertahanan negara.

Pasal 7

Fungsi identifikasi Ancaman Siber untuk mengetahui:

a. jenis Ancaman Siber;
b. bentuk Ancaman Siber; dan
c. metode Ancaman Siber.

Paragraf 1

Jenis Ancaman Siber

Pasal 8

(1) Jenis Ancaman Siber sebagaimana dimaksud dalam Pasal 7 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.

(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 9

(1) Bentuk Ancaman Siber sebagaimana dimaksud dalam Pasal 7 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 yang disebabkan oleh kemajuan teknologi informasi dan sistem elektronik.

Paragraf 3
Metode Ancaman Siber

Pasal 10

(1) Metode Ancaman Siber sebagaimana dimaksud dalam Pasal 7 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* (DDoS) 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 yang 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 yang disebabkan oleh kemajuan teknologi informasi dan sistem elektronik.

Bagian Kedua
Klasifikasi Ancaman Siber

Pasal 11

Klasifikasi Ancaman Siber terhadap penyelenggaraan pertahanan negara terdiri atas:

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

b. Ancaman Siber 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 secara nyata akan melakukan kegiatan yang melanggar norma dan hukum, serta kaidah atau kontrol keamanan informasi serta aset fisik lainnya.

Pasal 13

(1) Sumber Ancaman Siber sebagaimana dimaksud dalam Pasal 12 mempunyai tujuan untuk mendapatkan keuntungan yang bersifat materil dan *immateril.*

(2) Sumber Ancaman Siber sebagaimana dimaksud pada ayat (1) dapat diidentifikasi 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 Siber merupakan segala sesuatu yang melatarbelakangi terjadinya ancaman dan Serangan Siber.
(2) Aspek Ancaman Siber sebagaimana dimaksud pada ayat (1) meliputi 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 PENGIDENTIFIKASIAN ANCAMAN SIBER

Bagian Kesatu
Mekanisme Identifikasi

Pasal 16

Mekanisme Pengidentifikasian Ancaman Siber merupakan cara kerja dalam proses meneliti, mencari, menemukan serta mencatat informasi dan data mengenai Ancaman Siber.

Pasal 17

Mekanisme identifikasi Ancaman Siber terdiri atas:
a. pemantauan anomali, *traffic*, dan log;
b. analisis awal untuk mengetahui jenis Ancaman Siber; dan
c. laporan secara berjenjang.

Pasal 18

(1) Pemantauan anomali, *traffic*, dan *log* sebagaimana dimaksud dalam Pasal 17 huruf a merupakan kegiatan memantau peristiwa keamanan siber dan memverifikasi

efektivitas tindakan perlindungan termasuk jaringan dan aktivitas fisik.

(2) Pemantauan anomali, *traffic*, dan *log* sebagaimana dimaksud pada ayat (1) dilakukan oleh Pranata Komputer Ahli Pertama secara terus-menerus.

(3) Hasil pemantauan anomali, *traffic*, dan *log* sebagaimana dimaksud pada ayat (1) dan ayat (2) dilaporkan kepada Kepala Sub Bidang Pemantauan, Analisis dan Pelaporan Bidang Operasi Siber Pushansiber Bainstrahan Kemhan untuk dilakukan analisis awal.

Pasal 19

(1) Analisis awal untuk mengetahui jenis Ancaman Siber sebagaimana dimaksud dalam Pasal 17 huruf b merupakan kegiatan analisa anomali untuk menentukan tingkat urgensi Ancaman Siber.

(2) Kegiatan analisis awal sebagaimana dimaksud pada ayat (1) dilakukan oleh Pranata Komputer Ahli Pertama, Kepala Sub Bidang Pemantauan, Analisis dan Pelaporan Bidang Operasi Siber Pushansiber Bainstrahan Kemhan.

Pasal 20

Laporan secara berjenjang sebagaimana dimaksud dalam Pasal 17 huruf c merupakan proses pelaporan dokumentasi hasil analisis awal sebagai referensi untuk tindaklanjut terhadap Ancaman Siber yang dilaksanakan secara hirarki mulai dari Pranata Komputer Ahli Pertama sampai dengan Kepala Bidang Operasi Siber Pushansiber Bainstrahan Kemhan.

BAB IV
WEWENANG DAN TANGGUNG JAWAB

Pasal 21

(1) Wewenang dan tanggung jawab dalam Pengidentifikasian Ancaman Siber dilaksanakan oleh Tim Monitoring.

(2) Tim monitoring sebagaimana dimaksud pada ayat (1) terdiri atas:
   a. Pranata Komputer Ahli Pertama;
   b. Kepala Sub Bidang Pemantauan, Analisis dan Pelaporan Bidang Operasi Siber Pushansiber Bainstrahan Kemhan; dan
   c. Kepala Bidang Operasi Siber Pushansiber Bainstrahan Kemhan.

Pasal 22

(1) Pranata Komputer Ahli Pertama sebagaimana dimaksud dalam Pasal 21 ayat (2) huruf a mempunyai tugas merencanakan, menganalisis, merancang, mengimplementasikan, mengembangkan dan atau mengoperasikan sistem informasi berbasis komputer.

(2) Kepala Sub Bidang Pemantauan, Analisis dan Pelaporan sebagaimana dimaksud dalam Pasal 21 ayat (2) huruf b mempunyai tugas melakukan

penyiapan bahan penyusunan kebijakan teknis dan pelaksanaan pemantauan, analisis, dan pelaporan aktivitas siber serta pembentukan *computer emergency response team* dalam rangka merespon Serangan Siber.

(3) Kepala Bidang Operasi Siber Pushansiber Bainstrahan Kemhan sebagaimana dimaksud dalam Pasal 21 ayat (2) huruf c mempunyai tugas melaksanakan penyiapan operasi siber meliputi pemantauan, analisis, dan pelaporan Ancaman Siber, penindakan, digital *forensic* dan pemulihan serta pembentukan *computer emergency response team.*

Pasal 23

Tim monitoring sebagaimana dimaksud dalam Pasal 21 bertugas melindungi infrastruktur informasi vital, sistem elektronik, informasi elektronik dan data elektronik yang berlokasi di:

a. kompleks Kemhan Merdeka Barat;
b. kompleks Kemhan Budi Kemuliaan;
c. kompleks Kemhan Salemba;
d. kompleks Kemhan Tugu Tani;
e. kompleks Kemhan Pondok Labu;
f. kompleks Kemhan Bintaro;
g. kompleks Kemhan Sentul;
h. kompleks Kemhan Rumpin;
i. kompleks Kemhan Cawang; dan
j. kompleks Kemhan lainnya yang memiliki sistem elektronik vital.

Pasal 24

Tim monitoring sebagaimana dimaksud dalam Pasal 21 mengamankan informasi elektronik dan data elektronik pertahanan negara yang meliputi:

a. data strategi pertahanan;
b. data sistem perencanaan pembangunan pertahanan;
c. data potensi pertahanan negara;
d. data pembangunan kekuatan pertahanan negara;
e. data sarana dan prasarana pertahanan;
f. data penelitian dan pengembangan pertahanan;
g. data pendidikan dan latihan Kemhan; dan
h. data keuangan Kemhan.

BAB V
PENGENDALIAN DAN PENGAWASAN

Pasal 25

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

Pasal 26

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

BAB VI
KETENTUAN PENUTUP

Pasal 27

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