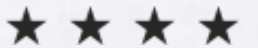




Id-SIRTII



NATIONAL INFOSEC COUNCIL



“Strategic Road Map to Securing National Information
Resources”

LEMBAGA NISC

DASAR HUKUM

- Keputusan Presiden: membentuk lembaga baru yang permanen (Dewan atau Badan); di luar negeri sebagai contoh al.: Malaysia Cyber Security, Jepang National Information Security Center
- Keputusan Presiden: memperluas kewenangan lembaga yang sudah ada (misalnya Dewan TIK Nasional) dengan status yang permanen dan memiliki kemampuan operasional secara teknis
- Undang Undang Informasi dan Transaksi Elektronik (ITE) dan Undang Undang Telekomunikasi dll. Peraturan Pemerintah (PP)
- RUU Keamanan Negara, RUU Konvergensi, RUU TIRITI dll

STRUKTUR ORGANISASI

- Ketua: Presiden Republik Indonesia
- Ketua Harian: Menteri Komunikasi dan Informatika
- Wakil Ketua: Menteri Pertahanan dan Keamanan
- Anggota: Menteri Hukum dan HAM, Menteri Keuangan, Menteri Dalam Negeri, Menteri Perdagangan, Menteri BUMN, Menteri Pendidikan, Menteri Perindustrian, Menteri ESDM, Menteri Perhubungan, Kapolri, Jaksa Agung, PPATK dll. dsb.

TUGAS POKOK

- Menyusun blue print dan road map keamanan informasi nasional
- Menyusun regulation framework (koridor regulasi) nasional
- Melakukan pengawasan dan penilaian terhadap:
 - Pembuatan regulasi keamanan informasi di setiap sektor strategis
 - Memastikan kepatuhan setiap organisasi terhadap regulasi
 - Memastikan telah diterapkannya standar keamanan informasi

TUGAS POKOK

- Melaporkan kepada Presiden hasil evaluasi setiap sektor pada setiap tahapan road map dan periode tertentu (3 bulan)
- Melakukan percepatan penguatan infrastruktur hukum dan penegakkan hukum terkait keamanan informasi nasional
- Melakukan koordinasi nasional untuk mensinergikan upaya pengamanan sumber daya informasi dan infrastrukturnya

ANGGARAN NISC

- Anggaran diambilkan dari Sekretariat Negara atau dianggarkan kepada departemen teknis terkait, misalnya Depkominfo
- Anggaran diperuntukkan:
 - Kegiatan Tim Ahli dan Tim Eksekutif
 - Penyelenggaraan operasional kantor sekretariat
 - Perumusan blue print dan regulation framework
 - Penyusunan road map implementasi setiap periode strategis

PENGGUNAAN ANGGARAN

- Melakukan penitaaian dan evaluasi periodik untuk setiap sektor
- Menyelenggarakan kegiatan kampanye, sosialisasi dan publikasi
- Program pembinaan sektor strategis (RAKERNAS, CEO Meeting, Executive Workshop, National Infosec Colaqioum & Exhibithion dll.)
- Mengadakan simposium Infosec Nasional & Internasional tahunan
- Penyusunan pelaporan dan penerbitan jurnal ilmiah, paper dll. yang akan menjadi acuan akademik dan basis pengetahuan Infosec di masa yang akan datang

ORGAN TEKNIKIS

INFRASTRUKTUR STRATEGIS

1. Sektor pemerintahan pusat dan daerah;
2. Sektor layanan publik pemerintah dan swasta;
3. Sektor pertahanan, keamanan dan ketertiban;
4. Sektor sumber daya alam, pertambangan dan energi;
5. Sektor perhubungan darat, laut/air dan udara;

6. Sektor keuangan, permodalan dan perbankan;
7. Sektor pelayanan pendidikan dan kesehatan;
8. Sektor perdagangan, perindustrian dan BUMN;
9. Sektor telekomunikasi, media dan penyiaran;
10. Sektor karya seni, budaya dan pariwisata;

INFRASTRUKTUR STRATEGIS

- Pemerintah dan layanan publik pusat dan daerah, Pertahanan dan keamanan serta ketertiban masyarakat, Pertambangan dan energi Transportasi, Keuangan, Pendidikan, Kesehatan, Perdagangan dan Industri, Telekomunikasi, media dan penyiaran, BUMN dll.
- Harus didefinisikan dengan jelas dan pasti sektor mana saja yang dianggap sebagai infrastruktur strategis. Tidak lebih dari 10
- Harus dibatasi ruang lingkup infratraktur strategis yang nantinya akan diamankan & dilaksanakan pencapaiannya secara bertahap

ID-SIRTII DAN APTEL

ORGAN TEKNIS NISC

- ID-SIRTII menyelenggarakan pengamanan infrastruktur melalui menyediakan berbagai layanan seperti monitoring, retensi logfile, laboratorium, pusat pelatihan dlsb. Yang bersifat shared services
- APTEL menyelenggarakan penerapan standarisasi pengamanan (SNI), pelatihan SDM, penguatan kelembagaan pemerintahan, menyusun tatanan industri CA, domain (CCTLD ID), standar dokumen terbuka, aplikasi dan layanan internet dlsb. Serta turut menjadi nara sumber penyusunan regulasi yang dilakukan NISC
- Anggaran operasional kedua lembaga ditanggung masing-masing Direktur Jenderal (ID-SIRTII oleh Deptel dan APTEL sendiri)

PERAN ID-SIRTII

- Lembaga teknis yang membantu setiap sektor untuk memenuhi standar pengamanan (compliance) yang ditentukan melalui:
 - Asistensi atau pendampingan implementasi sistem pengamanan
 - Menyelenggarakan pelatihan (sertifikasi) SDM yang diperlukan
 - Memberikan layanan monitoring dan pengamanan infrastruktur
 - Melibatkan sektor – sektor yang terkait ke dalam program atau sistem pengamanan yang diselenggarakan oleh ID-SIRTII

DASAR HUKUM UU 36/99

- Pada Pasal 4 ayat (1) pada Bab yang mengatur Pembinaan dinyatakan bahwa: Telekomunikasi dikuasai oleh Negara dan penmbinaannya dilakukan oleh Pemerintah
- Pasal 7 ayat (2) huruf a, untuk melindungi kepentingan dan keamanan Negara dimana kegiatan ini dilakukan melalui pemantauan, pendeteksian dini dan peringatan dini terhadap ancaman dan gangguan pada jaringan telekomunikasi berbasis protokol Internet di Indonesia
- Pasal 11. Izin diberikan oleh Menteri yang didelegasikan kepada Direktur Jenderal (Dirjen) – di bidang infrastruktur

DASAR HUKUM PP

52/2000

- Dalam PP 52/2000 tentang Penyelenggara Telekomunikasi dinyatakan bahwa Izin di berikan oleh Pemerintah melalui Menteri, yang diatur secara teknis dalam KM. 21/2000 tentang Penyelenggara Jasa Telekomunikasi yang kemudian diubah diperbaharui menjadi KM 30/2004
- Pasal 47 menyatakan bahwa bagi penyedia jasa telekomunikasi Izin di berikan oleh Direktur Jenderal. Menurut KM. 21/2000 tentang Penyelenggara Jasa Telekomunikasi pada pasal 1 angka 25 yang di maksud dengan Direktur Jenderal adalah Direktur Jenderal Pos dan Telekomunikasi yang membidangi infrastruktur

PERMEN 26/2007

- Tugas ID-SIRTII pengamanan jaringan Telekomunikasi berbasis Protokol Internet yang merupakan wewenang Dirjen Postel
- ID-SIRTII harus bekerjasama dengan Penyedia Jasa Internet
- Tugas pengamanan jaringan Telekomunikasi berbasis Protokol Internet yang berada di level Infrastruktur Internet, ID-SIRTII tidak berwenang & tidak kompeten menangani konten & aplikasi
- Menyimpan & menyediakan rekaman transaksi koneksi (logfile) untuk mendukung proses penegakan hukum sesuai kewajiban di dalam modern licensing penyelenggara jasa Internet

KEWENANGAN UTAMA

- Kegiatan utama ID-SIRTII yaitu Pemantauan, Pendeteksian dini & Peringatan dini terhadap ancaman & gangguan pada jaringan telekomunikasi berbasis protokol internet & membangun & atau menyediakan, mengoperasikan, memelihara & mengembangkan sistem database pemantauan & pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet, menyimpan rekaman transaksi (logfile) & mendukung proses penegakan hukum. Ini hanya dapat berjalan sepanjang kewenangan tersebut dikaitkan dengan pemberian izin bagi penyedia jasa (kewajiban pengamanan infrastruktur di dalam modern licensing), dimana kewenangannya ada pada Dirjen Postel.

PENYEDIAAN ALAT BUKTI

- Menunjang Proses pengakuan Hukum & Log File merupakan alat bukti yang menunjang proses penyidikan, penyelidikan & pemeriksaan di pengadilan. **Logfile hanya dapat di peroleh melalui penyedia Jasa telekomunikasi** dalam hal ini ISP (Penyedia Jasa Internet) yang Izinnya di berikan oleh Dirjen Postel sebagaimana di amanatkan oleh UU 36/1999 tentang Telekomunikasi & PP 52/2000 tentang Penyelenggara Telekomunikasi yang kemudian diatur dalam Keputusan Menteri Perhubungan Nomor KM 30 tahun 2004 tentang Perubahan atas Keputusan Menteri Perhubungan Nomor KM. 21 tahun 2000 tentang Penyelenggara Jasa Telekomunikasi

RUANG LINGKUP ID-SIRTII

Application Layer	Web, IRC, Mail	Users Service Level
Transport Layer	TCP/UDP	Protocol Level
Internet Layer	IP Address	Protocol Level
Data Link Layer	Mac Address	Operator Level
Physical Layer	Cable, Wireless	Operator Level

PENGAWAKAN ID-SIRTII

- Modal utama lembaga CERT/National CSIRT/CC agar dapat pengakuan (acknowledgement & trust) dari komunitas CERT / keamanan Internasional adalah kredibilitas, integritas, keahlian, independensi & **komitmen** untuk senantiasa konsisten berkarir di bidang security serta aktif dan proaktif dalam pergaulan tsb.
- SDM serta keahliannya adalah investasi terbesar lembaga CERT sehingga mempertahankan & melaksanakan regenerasi menjadi jauh lebih penting dibandingkan teknologi, fasilitas & peralatan
- Peningkatan kemampuan & pengalaman SDM harus dilakukan secara bertahap & berkelanjutan disertai **kepastian kariernya**

ID-SIRTII SEBAGAI EWS

- Menyelenggarakan sistem pemantauan nasional
 - Eksisting 11 sensor pada 9 NAP/ISP & 2 Exchange Nasional
 - Eksisting 3 sensor Tsubame Project (APCERT + JPCERT)
- Menyelenggarakan sistem pemantauan lokal
 - Tim Respon Insiden di setiap provinsi (UPT) Ditjen Postel
 - EWS di Data Center/Exchange/Gateway 33 provinsi/BTIP
- Pengamanan 10 infrastruktur kritis (strategis) – eksisting

IDSIRTII SEBAGAI CC

- Pusat Pelaporan Insiden Nasional / CC – Tim Respon Insiden Infrastruktur Internet Indonesia
- Single point of contact (proposed member FIRST, full member APCERT, acknowledge by ITU), untuk konstituen Industry (ISP, NAP), LEA, Community di Indonesia
- Perlu kewenangan melakukan mitigasi insiden, preemtive action (surveillance, filtering), countermeasure & recovery
- Usulan Peraturan Menteri yang baru – terlampir

ID-SIRTII CSIRT

- Kemampuan & kewenangan mitigasi insiden – draft RPM baru
- Memiliki fasilitas, fungsi Riset & Pengembangan untuk mitigasi
 - Lab. Simulasi Insiden (Drill Test) & Data Mining (cyberwarfare)
 - Lab. Honey Net (riset pola serangan) & Malware (riset malicious code)
 - Lab. Digital Forensic & Pusat Pelatihan (sertifikasi keahlian SDM)
- Menyelenggarakan penyimpanan & analisa log

PERAN REGULASI APTEL

- Lembaga yang menyusun framework, standar, regulasi, policy & road map implementasi pengamanan informasi setiap sektor:
 - Asistensi atau pendampingan implementasi standar pengamanan
 - Menyelenggarakan pelatihan (sertifikasi) SDM yang diperlukan
 - Melakukan evaluasi (compliance) terhadap implementasi standar pengamanan dan menguji keamanan informasi yang diterapkan
 - Melakukan pengkajian, studi banding untuk pengembangan standar, regulasi, policy & road map implementasi pengamanan informasi

RUANG LINGKUP APTEL

- Menyusun regulasi: Anti SPAM Act, Panduan Pengamanan Web, WiFi, Mail, Layanan Publik/Pemerintahan, Aplikasi Aman dlsb.
- Menyelenggarakan penerapan standarisasi pengamanan (SNI), pelatihan SDM, penguatan kelembagaan pemerintahan dlsb.
- Menyusun tatanan industri CA, Domain (CCTLD ID), standar dokumen terbuka, aplikasi dan layanan internet dlsb.
- Pengendalian content: layanan white list & black list, panduan pengamanan konten negatif, sosialisasi, penyebaran aplikasi dlsb

APTEL GOVCERT

- Tim Respon Insiden Pemerintah, pengamanan dan mitigasi
- Asistensi & fasilitasi pembentukan Local GOVCERT
- Koordinasi penanganan insiden dengan Local GOVCERT
- National Infosec Help Desk (hotline) pemerintah (DETIKNAS)
- PPNS dalam proses penegakan hukum di dalam UU ITE 8/2008

APTEL SHARED SERVICES

- Lembaga akreditasi penyelenggaraan CA (potensi PNBPN)
- Lembaga akreditasi penyelenggaraan SNI (potensi PNBPN)
- Lembaga pembina penyelenggaraan CCTLD (potensi PNBPN)
- Layanan pengendalian konten negatif (Dewan Konten)

DETIKNAS/MENKOMINFO

DIRJEN PENYELENGGARAAN	DIRJEN APLIKASI INFORMATIKA
DIR. TELEKOMUNIKASI Concern: Industry, Critical Infrastr.	DIR. KEAMANAN INFORMASI Concern: Government, Critical Infr.
National CSIRT/CC, Pusat Pelaporan Insiden Nasional, Single Point Contact, Mitigasi, Recovery, Preemptive, Counter	GOVCERT, Infosec Help Desk, Audit E-Gov Infosec, Asistensi Pembentukan Local GOVCERT, GOV Compliance
Lab. R & D, Log Retention & Analysis, Shared Services untuk Industri & LEA`	Regulasi, Standarisasi (SNI), Tatahan Industri Aplikasi (CA, CCTLD), Content Regulation (Dewan Konten)
Local Internet Infrastructure EWS 33 Provinsi (di Local	Local GOVCERT 33 Provinsi (Dinas / Badan Kominfo/PDF)

ID-SIRTII

- Ravindo Tower 17th Floor
- Kebon Sirih Raya, Kav. 75
- Central Jakarta, 10340
- Phone +62 21 3192 5551 ; Fax +62 21 3193 5556
- office@idsirtii.or.id ; www.idsirtii.or.id
- We look forward for future cooperation with you all.
Thank you.