

PERANAN PEMERINTAH DALAM PENGAMANAN INTERNET INDONESIA



**DITJEN POS DAN TELEKOMUNIKASI
DEPARTEMEN KOMUNIKASI DAN
INFORMATIKA**

DAFTAR ISI



- **LATAR BELAKANG**
- **PEMBENTUKAN LEMBAGA KEAMANAN JARINGAN INTERNET**
- **ASPEK LEGAL KEWAJIBAN PENGAMANAN JARINGAN INTERNET**
- **ASPEK TEKNIS PENUNJANG KEWAJIBAN PENGAMANAN JARINGAN INTERNET**

LATAR BELAKANG



PERLUNYA PENGAMANAN INTERNET



1. Pemanfaatan internet di Indonesia berkembang secara sangat pesat sejalan dengan manfaat yang ditawarkan dan diperoleh oleh masyarakat melalui berbagai aplikasi dan penerapannya.
2. Profile keamanan internet di Indonesia: 30 juta pemakai aktif/hari, 10 Gbits/s jumlah trafik nasional, 1 juta serangan/hari, 56% sangat tinggi resiko kena serangan dan 3 serangan yang paling sering: web defacement, phishing, SQL database exploits, serta 3 hal yang menjadi kelemahan keamanan: kurangnya kebijakan kewanaman perusahaan, terbatasnya pengetahuan tentang keamanan, kurang bagus nya kualitas design web/application
3. Sejalan dengan fenomena ini dan semakin tergantung nya kegiatan masyarakat terhadap internet, maka value dari internet pun bertambah tinggi, yang menyebabkan meningkat nya sejumlah resiko yang dihadapi masyarakat banyak baik dalam kegiatan ekonomi, politik, sosial budaya dan pertahanan keamanan.
4. Masing-masing negara mengambil inisiatif untuk mengamankan infrastruktur internet nya melalui berbagai cara, salah satunya dengan memberlakukan *cyberlaw* dan mendirikan lembaga semacam CSIRT/CERT untuk mengawasi keamanan internet di “wilayah”-nya masing-masing.

AMANAT PENGAMANAN INTERNET DALAM PERUNDANG-UNDANGAN/PERATURAN



- **Amanat UU 36 Tahun 1999 pasal 39.**

Penyelenggara telekomunikasi wajib melakukan pengamanan dan perlindungan terhadap instalasi dalam jaringan telekomunikasi yang digunakan untuk penyelenggaraan telekomunikasi. Ketentuan pengamanan dan perlindungan sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

- **Peraturan Pemerintah No. 52 Tahun 2000 pasal 82.**

Setiap jaringan telekomunikasi, sarana dan prasarana telekomunikasi harus dilengkapi dengan sarana pengamanan dan perlindungan agar terhindar dari gangguan telekomunikasi.

PEMBENTUKAN LEMBAGA KEAMANAN JARINGAN INTERNET



DUKUNGAN PEMERINTAH DALAM PENANGANAN KEAMANAN JARINGAN INTERNET



- Kasus atau *incident* yang menimpa sistem informasi dan teknologi pendukung pemilu 2004 di Indonesia membuka mata masyarakat akan besarnya ancaman keamanan yang dapat menimpa berbagai sistem berskala nasional apapun yang ada di tanah air.
- Dengan kesepakatan bersama (MoU) antara Mastel, APJII, Awari dan Dirjen Jenderal Pos dan Telekomunikasi maka diperlukan adanya dukungan terhadap pemanfaatan jaringan telekomunikasi berbasis protokol internet yang relatif aman dari ancaman dan gangguan.
- Untuk mendukung pemanfaatan jaringan telekomunikasi berbasis protokol internet yang relatif aman dari ancaman dan gangguan maka dibuatlah :

Peraturan Menteri Komunikasi dan Informatika Nomor 26/PER/M.KOMINFO/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

TUJUAN PENGAMANAN INTERNET



- Tujuan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet :
 - terlaksananya dukungan proses penegakan hukum;
 - terciptanya pemanfaatan jaringan telekomunikasi berbasis protokol internet yang aman;
 - terlaksananya koordinasi dengan pihak-pihak terkait baik di dalam maupun luar negeri.

RUANG LINGKUP PENGAMANAN JARINGAN INTERNET



- a. mensosialisasikan kepada seluruh pihak yang terkait untuk melakukan kegiatan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet;
- b. melakukan pemantauan, pendeteksian dini dan peringatan dini terhadap ancaman dan gangguan pada jaringan telekomunikasi berbasis protokol internet di Indonesia;
- c. membangun dan atau menyediakan, mengoperasikan, memelihara dan mengembangkan sistem database pemantauan dan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet sekurang-kurangnya untuk:
 - 1). mendukung kegiatan sebagaimana dimaksud dalam butir b;
 - 2). menyimpan rekaman transaksi (log file);
 - 3). mendukung proses penegakan hukum.
- d. melaksanakan fungsi layanan informasi atas ancaman dan gangguan keamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet;
- e. menyediakan laboratorium simulasi dan pelatihan kegiatan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet;
- f. melakukan pelayanan konsultasi dan bantuan teknis;
- g. menjadi contact point dengan lembaga terkait tentang pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet baik dalam negeri maupun luar negeri.

PEMBENTUKAN ID-SIRTII



- Untuk melaksanakan ruang lingkup pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet, berdasarkan Peraturan Menteri Komunikasi dan Informatika Nomor 26/PER/M.KOMINFO/5/2007 Pasal 5, perlu dibentuk lembaga tersendiri.
- Lembaga sebagaimana yang dimaksud adalah **Tim ID-SIRTII. (Indonesia Security Incident Response Team Internet Infrastructure)**

ASPEK LEGAL KEWAJIBAN PENGAMANAN JARINGAN INTERNET



KEWAJIBAN PENGAMANAN JARINGAN INTERNET OLEH PENYELENGGARA TELEKOMUNIKASI



Peraturan Menteri Komunikasi dan Informatika Nomor 26/PER/M.KOMINFO/5/2007 Pasal 19.

*Setiap penyelenggara yang menggunakan protokol internet **wajib melakukan rekaman transaksi koneksi (log file)** yang disampaikan ke system database pemantauan dan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet yang dimiliki oleh Pelaksana ID-SIRTII.*

KEWAJIBAN PENGAMANAN JARINGAN INTERNET OLEH NAP DAN IX



Peraturan Menteri Komunikasi dan Informatika Nomor 26/PER/M.KOMINFO/5/2007 Pasal 20.

*Pengelola Internet Exchange Point atau penyelenggara jasa interkoneksi internet (NAP) yang beroperasi di Indonesia **wajib mengaktifkan dan menyediakan fasilitas monitoring jaringan dan terhubung secara online** kepada system database pemantauan dan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet yang dimiliki oleh Pelaksana ID-SIRTII.*

KEWAJIBAN PENGAMANAN JARINGAN INTERNET OLEH PENGELOLA WARNET, HOTSPOT DAN SEJENISNYA



Peraturan Menteri Komunikasi dan Informatika Nomor 26/PER/M.KOMINFO/5/2007 Pasal 21.

*Pengelola Warnet, Hotspot, dan sejenisnya **wajib mendata setiap pengguna jasa internet** dalam rangka pengamanan pemanfaatan jaringan telekomunikasi berbasis internet dan wajib disimpan sekurang-kurangnya selama 1 (satu) tahun, sekurang-kurangnya meliputi :*

- a. **Identitas pengguna jasa internet***
- b. **Waktu mulai dan berakhirnya penggunaan akses internet***

*ISP yang menyelenggarakan jasa layanan pra bayar **wajib mendata identitas pengguna***

KEWAJIBAN SINKRONISASI



Peraturan Menteri Komunikasi dan Informatika Nomor 26/PER/M.KOMINFO/5/2007 Pasal 22.

*Setiap penyelenggara telekomunikasi yang menggunakan protokol internet **wajib melakukan penyelarasan waktu (clock synchronization)** sesuai dengan server yang ditetapkan oleh Direktur Jenderal.*

ASPEK TEKNIS PENGAMANAN JARINGAN INTERNET



TATA KELOLA PERANGKAT DETEKSI (MONITORING)



Peraturan Dirjen Postel Nomor 225/DIRJEN/2008 tentang Tata Kelola Perangkat Deteksi ID-SIRTII

***Perangkat Deteksi** adalah perangkat milik ID-SIRTII berfungsi memantau aktifitas lalu lintas jaringan internet penyelenggara untuk memberikan peringatan dini jika ada ancaman dan gangguan*

Hak Pemerintah :

- a. Menempatkan perangkat deteksi di NAP/IX*
- b. Mengoperasikan dan memelihara perangkat deteksi*
- c. Melakukan perbaikan dan upgrade*
- d. Melakukan pengawasan dan evaluasi*

Kewajiban Pemerintah :

- a. Membiayai pengadaan, instalasi, pengadaan, pemeliharaan dan perbaikan*
- b. Memberikan penjelasan atas aktifitas perangkat deteksi*

REKAMAN TRANSAKSI KONEKSI (LOG-FILE)



Peraturan Dirjen Postel Nomor 227/DIRJEN/2008 tentang Pedoman Pelaksanaan Rekaman Transaksi Koneksi (Log-File) dan Tata Cara Pelaporan Bagi Penyelenggara Jaringan Telekomunikasi Berbasis Protokol Internet

- *Rekaman aktifitas transaksi koneksi (log file) adalah suatu file yang mencatat akses pengguna pada saluran akses operator/ penyelenggara jasa akses berdasarkan **alamat asal protocol internet (source), alamat tujuan (destination), Jenis protocol yang di gunakan, port asal (source), Port tujuan (destination) dan waktu (time stamp) serta durasi terjadinya Transaksi.***
- *Rekaman transaksi dilakukan pada Gateway internasional, RAS, jaringan distribusi pelanggan, layanan akses melalui seluler, jaringan local peering, dll*
- *Tata cara pengiriman melalui online/offline*