PERTANYAAN YANG SERING DIAJUKAN
TENTANG RUANG LINGKUP TUGAS ID-SIRTII

1. Apa fungsi dan peran ID-SIRTII?

Indonesia – Security Incident Response Team on Information Infrastructure (disingkat ID-SIRTII) dibentuk oleh Menteri Komunikasi dan Informatika yang anggotanya terdiri dari unsur Pemerintah (termasuk penegak hukum), pakar di berbagai bidang terkait, akademisi, praktisi dan profesional di bidang telekomunikasi khususnya Internet. Fungsi utamanya adalah melakukan upaya pengamanan dan pemantauan infrastruktur Internet Nasional.

Peran pengamanan dan pemantauan dilakukan bersama dengan seluruh unsur penyelenggara infrastruktur dan jasa yang dipandang kompeten serta memiliki posisi strategis di dalam komunitas Internet Nasional. Aktivitas semacam ini juga diselenggarakan oleh lembaga sejenis di berbagai negara dan juga oleh otoritas Internet internasional. ID-SIRTII bekerjasama dengan berbagai lembaga sejenis di luar negeri melalui saluran formal antar pemerintahan.

Meskipun dibentuk oleh Menteri dan dibiayai oleh Negara, namun ID-SIRTII adalah lembaga yang idependen yang mengutamakan kepentingan publik. Keberadaan unsur Pemerintah lebih banyak berperan sebagai fasilitator, sedang fungsi teknis (yang membutuhkan keahlian spesifik dan profesional) dan kebijakan formal (untuk kepentingan publik) akan selalu dirumuskan bersama oleh anggota yang merupakan perwakilan pemangku kepentingan Internet Nasional.

2. Bagaimana tata cara pelaksanaan pengamanan tersebut?

Sebagaimana lembaga CERT/CSIRT di luar negeri, ID-SIRTII menjalankan fungsi monitoring pada sejumlah simpul utama jaringan Internet Nasional. Tujuan dari monitoring adalah untuk deteksi dini (early warning system) adanya potensi gangguan, ancaman, kemungkinan serangan terhadap infrastruktur Internet.

Pada dasarnya yang dipantau adalah pola (pattern) tertentu dari traffic Internet yang sedang berlangsung. Perangkat sensor yang dipasang memiliki teknologi identifikasi berdasarkan database pattern untuk mendeteksi traffic yang dianggap berbahaya. Bila diketahui ada aktivitas mencurigakan maka sistem pemantauan akan memberi peringatan agar ditindaklanjuti.

Perangkat sensor ditempatkan pada core network sejumlah NAP dalam mode pasif. Artinya, perangkat sensor ini tidak memungkinkan untuk melakukan intervensi terhadap traffic yang sedang aktif.

Fungsi pemantauan dimaksudkan sebagai upaya preventif, mencegah terjadinya kemungkinan serangan akibat aktifitas tidak sah di Internet. Lebih jauh, fungsi ini diharapkan mampu memberikan early warning (peringatan dini) terhadap infrastruktur Internet nasional dan yang bersifat kritis (misalnya perbankan, keuangan, transportasi, energi dan pemerintahan / layanan publik) sehingga dapat melakukan tindakan yang diperlukan untuk mencegah dan menanggulangi.

Selain fungsi pemantauan, ID-SIRTII melakukan pengumpulan rekaman transaksi koneksi (log). Pengumpulan ini dimaksudkan sebagai alat bantu analisa dan alat bukti bagi proses penyidikan dan penindakan hukum (law enforcement) bila terjadi tindak pidana atau pelanggaran hukum lainnya. Proses rekaman transaksi koneksi (log) dilakukan sendiri oleh ISP, kemudian dikirimkan ke ID-SIRTII dalam format terenkripsi untuk kemudian langsung disimpan dan diamankan.

Perekaman transaksi koneksi (log) inipun tidak mencakup keseluruhan informasi traffic hingga sampai ke konten melainkan hanya meliputi sebagian informasi layer transport (sesuai standar TCP/IP Layer) yaitu antara lain:

1. IP address (alamat IP, identitas Internet);
2. Jenis protocol akses (TCP, UDP, HTTP, FTP, SMTP);
3. Alamat port asal (source) maupun tujuan (destination);
4. Waktu (time stamp) yang lamanya diakumulasikan (durasi).

Sehingga jelas bahwa content (isi) dan atau kandungan data transaksi Internet, BUKAN bagian yang akan dipantau ID-SIRTII dan atau dicatat dalam rekaman transaksi koneksi oleh ISP. ID-SIRTII juga TIDAK AKAN MELAKUKAN PERUBAHAN APAPUN terhadap asal, identitas, tujuan, kandungan dan catatan waktu transaksi yang dipantau oleh sistem pemantauan maupun yang dicatat di dalam log.

Rekaman transaksi koneksi Internet ini dapat dianalogikan seperti catatan billing (tagihan) telepon yang hanya mencatat alamat asal dan tujuan panggilan telepon atau SMS serta jangka waktu (durasi) pemakaian. Sedangkan isi percakapan serta SMS tidak ditampilkan. Pada prinsipnya rekaman transaksi koneksi Internet sama atau mirip dengan bentuk catatan billing (tagihan) telepon tersebut.

3. Apakah aktivitas ini tidak melanggar privacy?

Pemerintah dalam hal ini Departemen Kominfo, Ditjen Postel/ID-SIRTII dan aparat penegak hukum (polisi, jaksa) yang terlibat dalam aktivitas ini, menghargai hak asasi, kebebasan dan kerahasiaan Individu yang dijamin oleh konstitusi. Semua hak warga negara terkait aktivitas ini dilindungi secara proporsional.

Namun bila terjadi tindak pidana atau pelanggaran hukum, Pemerintah memiliki otoritas, kewenangan untuk memanfaatkan segala sumber daya untuk melakukan penegakan (enforcement). Maka data yang ada pada ID-SIRTII dapat digunakan untuk maksud penegakan hukum dan hal ini bukan merupakan pelanggaran terhadap privacy. Prosedurnya mengikuti ketentuan hukum yang berlaku

4. Siapa saja yang dikenai kewajiban ini?

Kewajiban ditujukan pada operator infrastruktur dan penyelenggara jasa layanan Internet. Yaitu operator telekomunikasi, NAP (Network Access Provider – penyelenggara infrastruktur jaringan, interkoneksi dan akses Internet internasional) dan ISP (Internet Service Provider – penyedia jasa dan layanan Internet). Termasuk penyelenggara akses Internet publik yang merupakan distribution channel (saluran distribusi layanan), seperti Warnet dan HotSpot.

Saluran distribusi layanan dikenai kewajiban karena digunakan masyarakat luas (publik) secara bebas sehingga tidak teridentifikasi. Pengguna layanan Warnet dan HotSpot sebagian besar anonim, bukan pelanggan yang tercatat (terdokumentasi) identitasnya sehingga tidak mudah diidentifikasi. Pengguna Warnet dan sejenisnya memiliki mobilitas tinggi (sering berpindah), tidak terikat pada satu penyelenggara layanan saja. Sifat akses anonim dan acak ini sering dimanfaatkan pelaku tindak pidana dan atau pelanggar hukum dalam menjalankan aksinya.

Kewajiban pengamanan juga berlaku bagi penyelenggara jaringan dan layanan Internet yang bersifat private atauclosed group (kelompok tertutup). Termasuk dalam klasifikasi ini adalah coporate (perusahaan) besar yang memiliki jaringan dan akses Internet sendiri serta memiliki banyak pengguna yang tersebar, juga jaringan lembaga pendidikan dan jaringan pemerintahan (pusat dan daerah).

Khusus untuk operator telekomunikasi, NAP dan ISP (dan sejenisnya), termasuk kelompok tertutup wajib melakukan pemantauan dan menyerahkan catatan (log) aktivitas dan transaksi jaringan secara periodik kepada ID-SIRTII untuk disimpan.

5. Apakah yang dimaksud dengan infrastruktur Internet?

Yang dimaksud dengan infrastruktur Internet adalah : jaringan pada layer fisik, jaringan secara logik pada layer data link, layer Internet dan layer transport pada TCP/IP Stack. Layer aplikasi bukan termasuk definisi infrastruktur.

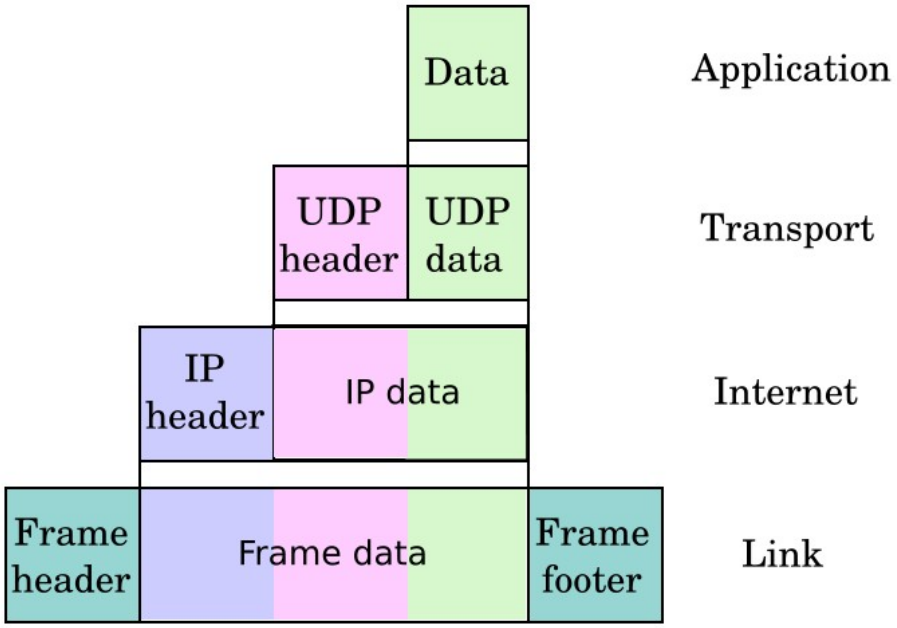

Diagram TCP/IP Stack

6. Apa yang dimaksud ancaman terhadap infrastruktur Internet?

Ancaman adalah semua upaya tidak sah yang berpengaruh langsung terhadap kelangsungan infrastruktur Internet. Yang antara lain mengakibatkan kelumpuhan

perangkat dan jaringan seperti DDOS, berubahnya arah lalu lintas data (hijacking) dan pemalsuan alamat (spoofing) dsb.

7. Defacing, spam, phising, malware termasuk ancaman infrastruktur?

Defacing pada umumnya diakibatkan oleh kelemahan sistem operasi dan aplikasi web. Spam juga diakibatkan oleh kelemahan pada aplikasi email. Sedangkan phising dan spyware terjadi karena kelemahan Operating System dan aplikasi Internet (email, web) dan perilaku pengguna. Virus dan trojan diakibatkan kelemahan perangkat lunak sistem operasi, aplikasi, konten dan perilaku pengguna. Semua dapat disebut sebagai ancaman keamanan komputer, berada pada layer aplikasi dan level pengguna (lihat TCP/IP Stack).

Insiden keamanan infrastruktur Internet, juga bisa diakibatkan oleh kelemahan sistem operasi dan kesalahan konfigurasi aplikasi perangkat. Bedanya sistem operasi ini bukan berfungsi mengelola konten atau sebagai interface bagi pengguna (aplikasi), melainkan digunakan mengatur lalu lintas data dan layanan dalam infrastruktur operator. Pada TCP/IP Stack insiden keamanan infrastruktur Internet terjadi pada level protokol dan operator (penyelenggara).

ID-SIRTII tidak menangani insiden keamanan komputer seperti spam, virus, trojan, spyware, malware dan deface yang menimpa komputer individual pengguna atau jaringan tertentu. Artinya tindakan mitigasi (antisipasi, penanggulangan dan perbaikan) dilakukan sendiri oleh tiap individu atau institusi yang mengalami masalah. ID-SIRTII hanya akan memberi peringatan dini dan bantuan teknis lainnya seperti pedoman serta prosedur mitigasi, penyediaan tools.

Kecuali apabila ada bukti teknis yang menunjukkan bahwa serangan itu berpotensi atau bagian upaya sistematis untuk menimbulkan gangguan dan kelumpuhan infrastruktur Internet. Dengan kata lain ID-SIRTII hanya menangani insiden yang secara langsung menimbulkan ancaman terhadap infrastruktur Internet.

8. Mengapa ID-SIRTII tidak menangani layer aplikasi?

Pertama, kewenangan ID-SIRTII dibatasi oleh Peraturan Menteri Kominfo Nomor 27/PER/M.KOMINFO/9/ 2006 Tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

Kedua, fokus ID-SIRTII adalah infrastruktur Internet, bukan konten. Penanganan layer aplikasi akan terkait erat dengan masalah filtering konten. Hal ini masih akan menimbulkan kontroversi terkait masalah perlindungan privacy dan kepercayaan publik karena belum diterbitkan aturannya.

Ketiga, teknologi filtering dan proteksi konten membutuhkan sumber daya sangat besar, investasi dan biaya operasional yang tidak sedikit. Filter konten pornografi dan anti spam misalnya, akan membutuhkan kemampuan komputasi paralel dan kapasitas memori sangat besar dan perangkat dalam jumlah yang sangat banyak di setiap tingkat distribusi operator Internet.

9. Siapa lembaga yang menangani ancaman keamanan komputer?

Penanganan masalah keamanan komputer, pada umumnya lebih banyak ditangani oleh pengguna atau perusahaan penyedia aplikasi keamanan komputer. Sedang masalah keamanan infrastruktur umumnya ditangani oleh operator.

Lembaga Pemerintah yang menangani keamanan komputer dan Internet belum ada. Sedangkan ID-SIRTII dimaksudkan sebagai lembaga independen (dengan Pemerintah sebagai fasilitator) yang akan menangani keamanan infrastruktur Internet dalam ruang lingkup terbatas seperti dijelaskan di atas.

Sebelumnya pernah dikenal organisasi independen inisiatif komunitas yaitu CERT (Computer Emergency Response Team). Organisasi ini memberikan edukasi, solusi penanganan dan pencegahan insiden keamanan komputer.

Seiring dengan popularitas Internet, CERT berkembang, ikut menangani insiden kemanan jaringan Internet. ID-SIRTII dapat dianggap sebagai adalah salah satu CERT. Di setiap negara ada beberapa organisasi sejenis yang umumnya berasal dari inisiatif gabungan Pemerintah dan komunitas.

Apabila nanti dikemudian hari telah semakin banyak tumbuh berbagai organisasi CERT/CSIRT, maka ID-SIRTII akan memposisikan diri sebagai CC (Coordination Center) dan single point of contact internasional.