PERTANYAAN YANG SERING DIAJUKAN
TENTANG IMPLEMENTASI TEKNIS ID-SIRTII

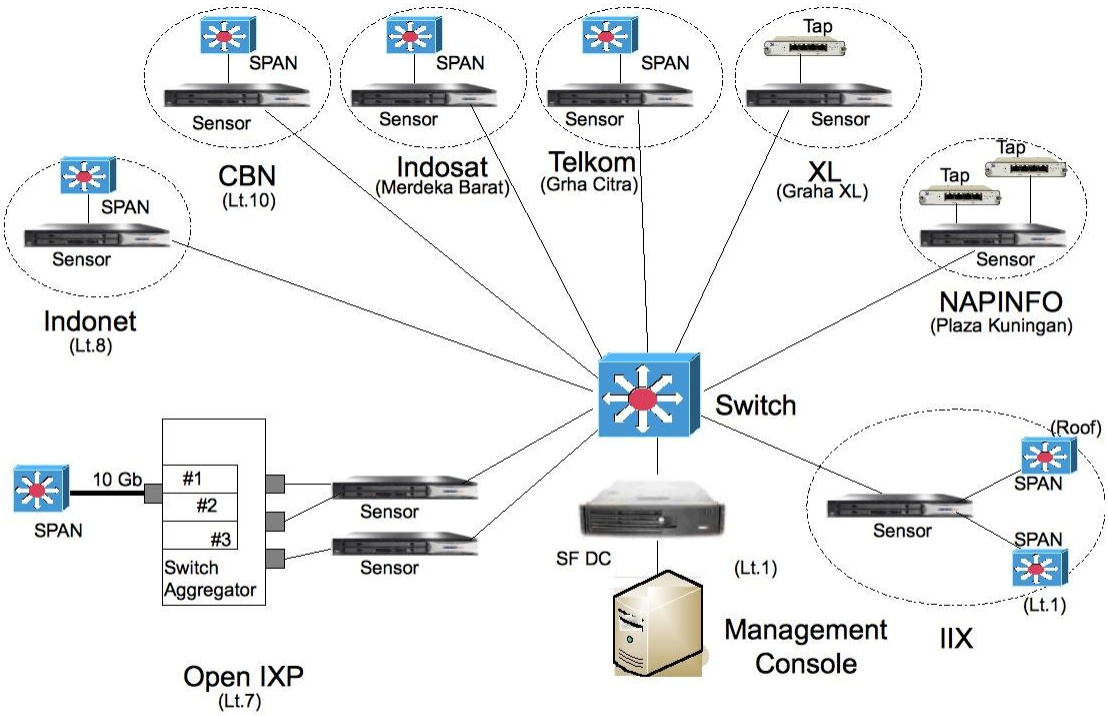
Apa saja kewajiban Penyelenggara?

Sesuai Peraturan Menteri Kominfo Nomor 27/PER/M.KOMINFO/9/2006 Tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet, dikenakan kewajiban pemantauan aktivitas (monitoring), perekaman catatan transaksi koneksi (log), sinkronisasi waktu (NTP) pada:

1. Operator (Penyelenggara Infrastruktur);
2. Penyelenggara Network Access Point (NAP);
3. Penyelenggara Exchange Point (IXP);
4. Penyelenggara Jasa Internet (ISP).

Bagaimana teknis implementasi Pemantauan Aktivitas Internet?

Pemantauan (monitoring) aktivitas Internet dilaksanakan dengan cara penempatan sejumlah perangkat sensor pada gateway utama NAP. Jumlahnya akan menyesuaikan dengan ketersediaan anggaran dan tingkat kebutuhan seimbang dengan skala dan pertumbuhan Internet nasional yang perlu dipantau, terutama infrastruktur kritis.



Interkoneksi di Gedung Cyber

Perangkat sensor difungsikan secara pasif, tidak digunakan untuk melakukan tindakan preventif maupun defensif yang bersifat intervensi terhadap jaringan NAP. Sensor akan dihubungkan secara tidak langsung ke jaringan NAP melalui perangkat mirror, tidak secara inline. Sehingga, topologi ini akan menghilangkan resiko down time pada

saat instalasi maupun karena failure. Sensor juga dipasang di Internet Exchange.

Seluruh perangkat sensor dihubungkan ke pusat Management Console melalui saluran independen yang seluruhnya akan diadakan dan dibiayai oleh anggaran Pemerintah.

Segala biaya operasional yang timbul akibat penempatan perangkat sensor, seperti untuk kebutuhan pasokan daya listrik, penggunaan ruangan data center dan sewa rack space tidak akan ditagihkan kepada Pemerintah, melainkan ditanggung oleh NAP sebagai konsekunsi dari pelaksanaan kewajiban yang disebabkan oleh regulasi.

Bagaimana dengan Klausul Kerahasiaan Pelanggan?

Perangkat sensor yang dipasang tidak ditujukan dan tidak difungsikan untuk memata-matai atau menyadap data dan informasi rahasia milik pelanggan/pengguna maupun data milik perusahaan penyelenggara yang terkait.

Penempatan perangkat sensor bukanlah bentuk dari lawful interception melainkan sebagai bagian dari sistem deteksi dini (Early Warning System) nasional terhadap kemungkinan terjadinya penyebaran worm, trojan, virus maupun dikenalinya sejumlah kerawanan pada aplikasi dan layanan yang saat itu sedang berlangsung di dalam jaringan dan kemungkinan terjadinya ancaman, gangguan dan serangan terhadap infrastruktur Internet sehingga insiden dapat diantisipasi sejak dari awal. Nantinya NAP juga akan diberikan akses Dashboard Management Console sehingga dapat berperan serta memantau jaringannya sendiri.

Penempatan perangkat sensor adalah kelaziman di dalam dunia pengamanan Internet dan menjadi bagian dari prosedur operasional sebagaimana prosedur pemantauan kondisi jaringan dan layanan untuk menjaga kualitas layanan yang harus dilakukan penyelenggara, sehingga tidak perlu Klausul Kerahasiaan (Non Disclosure Agreement) tertentu karena bukan sesuatu yang bersifat rahasia.

Bagaimana teknis implementasi Rekaman Transaksi Koneksi?

Analogi rekaman transaksi koneksi (log) adalah catatan billing telepon yang berisi data dan informasi nomor telepon asal, tujuan dan waktu (mulai/berakhir, durasi) dari oanggilan telepon ataupun SMS. Isi dari percakapan telepon maupun SMS tidak perlu dicatat dan atau ditampilkan. Sehingga tidak diperlukan Klausul Kerahasiaan (Non Disclosure Agreement) tertentu untuk melindungi privacy.

Rekaman transaksi koneksi (log) yang disimpan di ID-SIRTII dilindungi dengan kunci rahasia (enkripsi) dan sesuai prosedur yang ditentukan oleh Pemerintah hanya dapat dibuka kembali untuk kepentingan penegakan hukum saja.

Rekaman transaksi koneksi (log) telah ditentukan formatnya, yaitu:

1. {source ip address} contoh 202.155.4.29;
2. {protocol} contoh TCP atau UDP;
3. {source port} contoh 35661;
4. {destination ip adress} contoh 203.144.3.109;
5. {destination port} contoh 80;

6. {date} DD/MM/YYYY contoh 22/01/2007;
7. {time stamp} HH:MM:SS contoh 23:15:02.

Khusus untuk rekaman transaksi koneksi (log) server otentikasi pengguna atau RAS (Remote Access Service) misalnya RADIUS, ditambahkan data:

1. {username} contoh mangkuprojo;
2. {code line identifier} contoh 021 7919000;
3. {date} contoh 22/01/2007;
4. {time stamp – durasi} contoh start 02:37:09 end 04:12.11.

Data perekaman (log) disimpan dalam bentuk digital dengan format file text comma separated (.csv). Untuk menghemat kapasitas media penyimpan. Sata ini dapat dikompresi sesuai kebutuhan dengan tanpa menghilangkan informasi yang telah terkandung di dalamnya.

Lebih lanjut dapat dipelajari Pedoman Pelaksanaan Rekaman Transaksi Koneksi (Log File) dan Tata Cara Pelaporan Bagi Penyelenggara Jaringan Telekomunikasi Berbasis Protokol Internet diatur dalam Peraturan Direktur Jenderal Pos dan Telekomunikasi Nomor 227/DIRJEN/2007.

Bagaimana proses pengiriman Log File?

Pengiriman Log File ke ID-SIRTII melalui beberapa alternatif:

1. Secara online ke server ID-SIRTII, baik real time (streaming) maupun periodik (perhatikan bagian lampiran Perdirjen 227/2007);
2. Secara offline ke ID-SIRTII dengan menggunakan format dan media digital (CD/DVD) dengan jadwal maksimal per 14 (empat belas) hari;
3. Setiap pengiriman akan dilindungi dengan kunci rahasia (enkripsi) serta kode pemeriksaan integritas data (checksum).

Selain diserahkan ke ID-SIRTII, data pencatatan (log) juga harus disimpan sendiri sebagai backup oleh Operator, NAP, IXP dan ISP sekurang-kurangnya selama 3 (tiga) bulan setelah diserahkan.

Lebih lanjut dapat dipelajari Pedoman Pelaksanaan Rekaman Transaksi Koneksi (Log File) dan Tata Cara Pelaporan Bagi Penyelenggara Jaringan Telekomunikasi Berbasis Protokol Internet diatur dalam Peraturan Direktur Jenderal Pos dan Telekomunikasi Nomor 227/DIRJEN/2007.

Bagaimana dengan teknis sinkronisasi waktu perangkat?

Seluruh perangkat jaringan Operator, NAP, IXP dan ISP wajib melakukan sinkronisasi waktu ke NTP server yang ditentukan oleh Direktur Jenderal Pos dan Telekomunikasi yaitu kelompok server **id.pool.ntp.org**. Operator, NAP, IXP dan ISP menyediakan server NTP untuk keperluan sinkronisasi waktu bagi seluruh perangkat jaringan yang berada di bawahnya (hingga tingkat pelanggan akhir) dan mewajibkannya. Sedang wilayah waktu menyesuaikan GMT yaitu GMT +7 untuk Waktu Indonesia Bagian Barat, GMT +6 untuk Waktu Indonesia Bagian Tengah dan GMT +5 untuk Waktu

Indonesia Bagian Timur.

Apa isi Klausul Kerjasama/Persetujuan Pelanggan terkait masalah ini?

Setiap Operator, NAP, IXP dan ISP wajib mencantumkan sejumlah ketentuan dalam PKS (Perjanjian Kerja Sama) dengan pelanggan dan atau dalam Klausul Persetujuan Pelanggan (Acceptance User Policy - AUP) pengguna di bawahnya seperti berikut:

1. Kewajiban melakukan sinkronisasi waktu perangkat jaringan dan terminal akses ke NTP server yang telah ditunjuk yaitu kelompok server **id.pool.ntp.org**;
2. Bagi pelanggan yang memiliki jaringan pengguna tertutup sendiri (private, closed user group) dan memiliki banyak pengguna serta tersebar, wajib melakukan perekaman transaksi koneksi (log) sendiri;
3. Bagi pelanggan yang memiliki jaringan pengguna tertutup sendiri (private, closed user group) dan memiliki banyak pengguna serta tersebar, wajib melakukan pendataan identitas pengguna layanannya;
4. Bagi saluran distribusi (seperti HotSpot dan Warnet) wajib menerapkan mekanisme otentikasi dan atau pendataan identitas pengguna.

Sanksi administratif dan teknis juga harus dicantumkan dalam setiap PKS (Perjanjian Kerja Sama) / Klausul Persetujuan Pelanggan sebagai berikut:

1. Penolakan dan atau pelanggaran terhadap kewajiban di atas dikenakan sanksi administrasi berupa teguran dan peringatan;
2. Penolakan dan atau pelanggaran terhadap kewajiban di atas dikenakan sanksi teknis berupa pemblokiran alamat Internet;
3. Bila sanksi administrasi dan teknis tidak diindahkan, maka kepada pengguna ybs. akan dikenakan pemutusan akses sementara;
4. Pemutusan akses (koneksi) dan pembatalan PKS untuk seterusnya.

Apakah yang dimaksud dengan kewajiban pendataan pengguna?

Sesuai Peraturan Menteri Nomor 27/PER/M.KOMINFO/9/2006 Tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet, dikenakan kewajiban pendataan pengguna kepada:

1. Pelanggan Operator, NAP, IXP dan ISP yang memiliki jaringan pengguna tertutup sendiri (private, closed user group) dan memiliki banyak pengguna serta tersebar. Termasuk dalam kategori ini adalah jaringan pendidikan dan pemerintahan (pusat dan daerah) yang aksesnya terbuka;
2. Saluran distribusi Operator, NAP, IXP dan ISP untuk akses publik seperti layanan HotSpot dan Warung Internet.

Data pengguna yang harus dicatat adalah:

1. Nomor kartu identitas (SIM, KTP, Kartu Pelajar/Mahasiswa);
2. Nama lengkap (opsional: nama kecil, julukan);
3. Alamat lengkap (opsional: nomer telepon, hp);
4. Jenis kelamin, Tanggal lahir, Pekerjaan, Status;
5. Catatan waktu akses (mulai, berakhir, durasi);

6. Catatan terminal akses dan IP yang digunakan;
7. Opsional: copy kartu identitas dan atau foto.

Penyelenggara jasa tidak dituntut untuk melakukan validasi data yang diberikan oleh pengunjung yang menggunakan layanannya. Data dicatat sesuai informasi dan identitas yang ditunjukkan secara apa adanya. Kesengajaan pemberian informasi dan identitas palsu oleh pengguna bukan menjadi tanggung jawab penyelenggara jasa.

Data pengguna disimpan sendiri oleh penyelenggara saluran distribusi dalam jangka waktu sekurang-kurangnya 1 (satu) tahun sejak terjadinya transaksi. Data akan diserahkan ke ID-SIRTII atau aparat penegak hukum apabila diminta (terjadi kasus).

Data pengguna disimpan dalam bentuk digital dengan format file text comma separated (.csv). Untuk menghemat kapasitas media penyimpan, data ini dapat dikompresi tanpa menghilangkan kandungan informasi yang telah ada di dalamnya.

Sedangkan data yang bersifat opsional (copy kartu identitas dan atau foto) disimpan dalam bentuk digital dengan format file citra (grafis) generik (.bmp, .tiff, .gif, .jpg atau .png) dengan ukuran aslinya (tidak terkompresi). Apabila tidak memungkinkan pendataan dengan format digital, maka dimungkinkan untuk melakukan pendataan dalam bentuk fisik (catatan atau copy).

Bagaimana bila penyelenggara akses publik menolak kewajiban tersebut?

Penolakan atau pelanggaran terhadap kewajiban dapat dikenakan sanksi administratif dan teknis sebagaimana diatur dalam PKS atau AUP dengan Operator, NAP, IXP dan ISP penyedia layanan di atasnya, yaitu berupa:

1. Sanksi administrasi, teguran dan peringatan;
2. Sanksi teknis, pemblokiran alamat Internet (IP adress);
3. Apabila sanksi administrasi dan teknis tidak diindahkan, maka pengguna ybs. akan dikenakan sanksi pemutusan akses (koneksi) dan pembatalan PKS;
4. Pemutusan akses (koneksi) dan pembatalan PKS.

Pidana juga dapat dikenakan sesuai dengan ketentuan peraturan perundangan lain yang berlaku, tergantung kepada kasus yang terjadi. Misalnya untuk kasus narkoba, maka sanksi pidana dikenakan berdasarkan UU Psikotropika dan KUHP. Demikian juga dengan kasus penipuan, penggelapan, perjudian, terorisme, pornografi, fraud, money laundry, trafficking, child abuse dsb. akan ditindak berdasarkan UU terkait dan KUHP. Artinya, sanksi pidana yang mungkin akan dapat dikenakan tidak hanya berdasarkan peraturan perundangan di bidang telekomunikasi saja.

Sanksi bagi penyelenggara jasa yang tidak melaksanakan kewajiban?

Pada dasarnya kewajiban ini adalah bagian dari upaya untuk meningkatkan kualitas pelayanan Internet secara nasional dan untuk memenuhi tuntutan pergaulan global. Masalah pengamanan Internet menjadi agenda penting di berbagai forum tingkat dunia (PBB, ITU) dan regional (Asia Pasifik, ASEAN). Sejumlah kesepakatan tingkat tinggi antar pemimpin negara dan regulator (kementerian) serta tingkat teknis antar lembaga CERT/CSIRT yang harus dilaksanakan oleh Indonesia.

Bagi para Operator, NAP dan ISP, sejumlah kewajiban di atas telah dinyatakan pada klausul komitmen (kesanggupan) di dalam Ijin Penyelenggaraan (modern licensing) yang telah diberikan Pemerintah (Menteri dan Dirjen Postel). Penolakan dan atau pelanggaran terhadap komitmen tersebut dapat dikenakan sanksi:

1. Administrasi, berupa teguran dan peringatan;
2. Administrasi, berupa pembekuan hingga pencabutan ijin;
3. Pidana berupa denda dan kurungan, sesuai dengan tingkat keterlibatan dalam kasus yang mungkin terjadi sebagai akibat tidak dilaksanakannya kewajiban.