Laporan Dwi Bulan IV 2014

Juli – Agustus 2014

ID-CERT[1]

Ringkasan
Di Laporan Dwi Bulan IV ini disajikan pengumpulan pengaduan selama dua bulan yaitu Juli dan Agustus 2014. Pengaduan tersebut diterima dalam bentuk email dan dikumpulkan sesuai kategori, sebagai bahan penyusunan statistik, dalam bentuk angka dan grafik. Spam, komplain spam, respon, network incident, Hak atas Kekayaan Intelektual, fraud, spoofing/phishing, dan malware merupakan kategori yang dipilih untuk pengelompokan pengaduan masuk.

Kata Kunci

Security – Pelaporan – Laporan Dwi Bulan

Daftar Isi

1. Pendahuluan

Bagian penting dari aktivitas sekarang adalah Internet. Pemakaian Internet sehari-hari kian menjadi lebih penting dari komunikasi antarwarga hingga transaksi bisnis multinasional, pengguna Internet kian banyak dan kian beragam – usia kanak-kanak sampai dengan para lansia, para pekerja di lapangan hingga *bot otomatis*. Batas-batas yang telah ada sebelumnya juga mengalami pergeseran dengan adanya Internet, menciptakan kemungkinan baru yang perlu dicermati. Tidak terkecuali aspek keamanan Internet (*Internet security*) yang menjadi perhatian secara khusus dan kerja sama banyak kalangan.

Sebagai bagian dari pemantauan keamanan Internet, ID-CERT menerima pengaduan lewat email yang diterima dari beberapa responden. Pengaduan tersebut dikelompokkan dalam sejumlah kategori dan disajikan dalam bentuk laporan Dwi Bulan. Laporan ini sebagai paparan gambaran insiden keamanan (*security incident*) yang terjadi selama dua bulan, Juli dan Agustus 2014.

[1] Indonesian Computer Emergency Response Team

Selain gambaran tersebut, penyediaan laporan ini juga dimaksudkan sebagai contoh data primer keamanan teknologi informasi (TI) di Indonesia.

Penting ditekankan dalam hal ini adalah tindak lanjut terhadap laporan tentang penyalahgunaan Internet (*Internet abuse*) sebagai respon positif dan langkah untuk memperbaiki keadaan. Hal ini juga bagian interaksi positif antara kita, pengguna Internet di Indonesia dengan pihak-pihak di mancanegara terkait penanganan laporan. Pengaduan yang diterima memberi gambaran bagian-bagian yang perlu dibenahi, keterkaitan antar lembaga, dan untuk membantu penyusunan rencana ke depan.

Pada laporan Dwi Bulanan IV 2014 ini, *spam* masih menempati jumlah pengaduan terbanyak yaitu mencapai 43,21%, sedangkan IPR menempati urutan pengaduan kedua dengan selisih sekitar 5% dari *spam* yaitu sebesar 37,95%. Dilihat dari sisi jumlah pengaduan, terdapat tiga kelompok besar: *spam* dan IPR pada kelompok pertama yang mencapai jumlah di atas 10.000 pengaduan, diikuti kelompok ke dua yang memiliki jumlah pelaporan sedang yaitu di bawah 10.000 namun di atas 1.000 laporan, dan kelompok terakhir berjumlah pengaduan rendah yaitu di bawah 1.000 pengaduan. Penjelasan lengkap tentang ketiga kelompok tersebut dipaparkan di bagian Uraian.

Pembuatan laporan ini berdasarkan pada data-data yang diperoleh dan diambil dari tiga puluh tujuh (37) responden yang terdiri dari: Kominfo, ID-CERT, PANDI, Detik.net, Zone-h dan Anti Fraud Command Center (AFCC), tiga operator telekomunikasi, tujuh NAP, dan 22 Penyedia Jasa Internet (PJI/ISP), Kemendikbud.

2. Metoda

Penyusunan dokumen Dwi Bulan ini mengambil data dari beberapa sumber dalam bentuk laporan dengan langkah-langkah berikut:

1. Pengambilan data dari sejumlah responden.
2. Penyusunan analisis berdasarkan :
   a) Tembusan laporan yang masuk lewat alamat email pengaduan penyalahgunaan (*abuse*) yang disediakan PJI/operator telekomunikasi/lembaga non-ISP.
   b) Tabulasi yang dikeluarkan oleh sejumlah responden. Tabulasi ini berupa kumpulan data yang telah dihitung dikelompokkan oleh responden

Dari laporan yang sudah terkumpul, dilakukan pengelompokan sebagai berikut:

Fraud Penipuan disengaja yang dibuat untuk keuntungan pribadi atau untuk merugikan individu lain[2] berdasarkan data yang sudah masuk ke penegak hukum.

Hak atas Kekayaan Intelektual Pengaduan tentang pelanggaran terhadap hasil karya yang terkait Undang Undang Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR)

Komplain Spam Keluhan/pengaduan email *spam* dari dalam negeri terhadap pengirim di Indonesia dan luar negeri

Malware Program komputer yang dibuat untuk maksud jahat[3].

Network Incident Aktivitas yang dilakukan terhadap jaringan pihak lain dan semua aktivitas terkait dengan penyalahgunaan jaringan.

[2] *Fraud*,
http://en.wikipedia.org/wiki/Fraud

[3] *Malware*,
http://en.wikipedia.org/wiki/Malware

Respon Respon terhadap laporan yang masuk.

Spam Penggunaan sistem pengolahan pesan elektronik untuk mengirim pesan-pesan tidak diharapkan dalam jumlah banyak, terutama untuk pengiklanan, tanpa pilih-pilih[4].

Spoofing/Phishing Pemalsuan email dan situs untuk menipu pengguna[5].

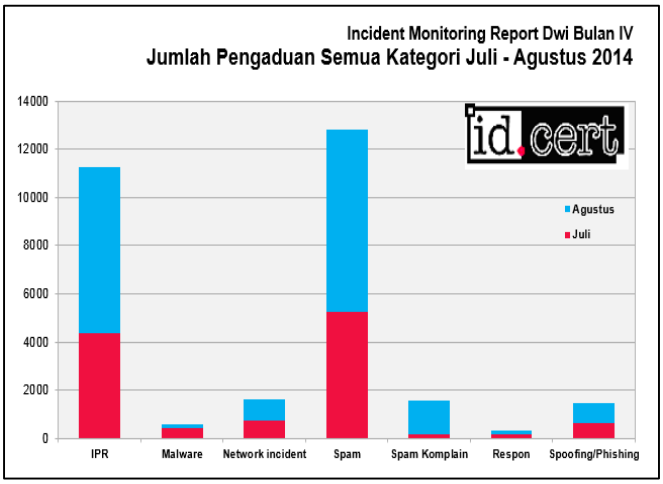
Lain-lain Laporan penyalahgunaan selain yang termasuk pada kategori yang di atas.

3. Uraian

Email pengaduan yang diterima dikumpulkan berdasarkan kategori pengaduan dan bulan, dengan demikian terdapat dua kelompok besar, bulan Juli dan Agustus 2014. Kategori pengaduan terdiri atas Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR), komplain spam, *malware*, *network incident*, respon, *spam*, dan *spoof*. Pengolahan data dilakukan dengan dua cara:

1. Penghitungan cacah dari tajuk (*header*) email, seperti bagian `From`, `To`, `CC`, dan `Subject`. Cara ini terutama digunakan untuk pengaduan dalam kondisi tidak mengikuti format baku yang biasanya dihasilkan perangkat lunak pelapor. Kategori pengaduan seperti *spam*, *spoof* biasanya termasuk jenis ini.
2. Penghitungan cacah dari isi email (*body*). Pengaduan *network incident* dan *malware* sebagai misal, menggunakan format pesan yang baku dan nama domain yang diadukan dapat diperoleh dari isi email pada bagian yang menggunakan format tertentu.

Grafik semua kategori *Incident Monitoring Report* untuk Dwi Bulan IV 2014 berdasarkan jumlah pengaduan per bulan ditampilkan pada Gambar 1.



Gambar 1 Jumlah pengaduan semua kategori Juli - Agustus 2014

Jumlah pengaduan masing-masing per bulan dan total dua bulan dapat dilihat lebih seksama di Tabel 1 dengan kategori pengaduan ditampilkan berdasarkan jumlah laporan yang diakhiri dengan Respon.

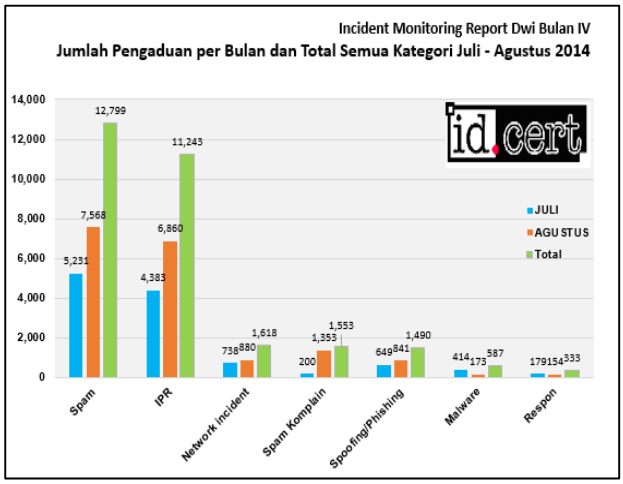
Tabel 1. Perkembangan jenis pengaduan selama Juli - Agustus 2014

Kategori	JULI	AGUSTUS	Total	%
Spam	5,231	7,568	12,799	43.21%
IPR	4,383	6,860	11,243	37.95%
Network incident	738	880	1,618	5.46%
Spam Komplain	200	1,353	1,553	5.24%
Spoofing/Phishing	649	841	1,490	5.03%
Malware	414	173	587	1.98%
Respon	179	154	333	1.12%

Pada Gambar 2 dapat dilihat perkembangan dari naik atau turunnya jumlah pengaduan antara bulan Juli dan Agustus 2014 dan jumlah total dua bulan.

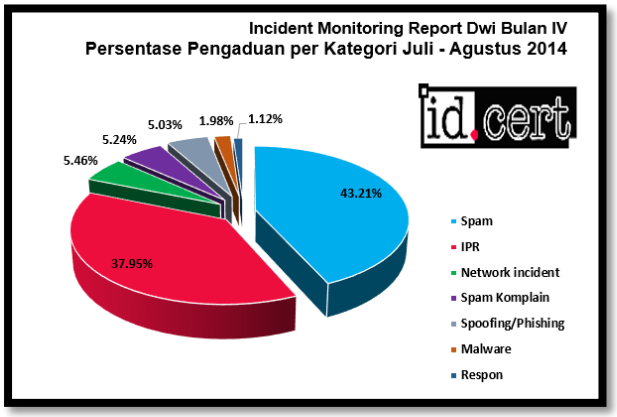
[4] *Spam (electronic)*, http://en.wikipedia.org/wiki/Spam_(electronic)

[5] *Spoofing attack*, http://en.wikipedia.org/wiki/Spoofing_attack



Gambar 2 Jumlah pengaduan per bulan dan total semua kategori Juli - Agustus 2014

Perhitungan perkembangan dilakukan terhadap jumlah pengaduan pada bulan pertama Juli, bulan kedua Agustus dan bernilai negatif jika terjadi penurunan. Secara umum tidak ada tren yang terjadi dari jumlah pengaduan Juli di banding Agustus karena masing-masing kategori ada yang meningkat yaitu *IPR*, *Network incident*, *spam*, *Spoofing/phising*, *Spam* Komplain tetapi ada pula yang menurun yaitu *Malware*. Persentase detail dari masing-masing dihitung terhadap jumlah pengaduan keseluruhan dapat dilihat pada Tabel 1. Tampilan tabel tersebut berdasarkan urutan persentase kategori dari yang terbanyak. Untuk melihat perbandingan besar persentase jumlah laporan antar semua kategori ditampilkan dalam bentuk diagram lingkaran yang disajikan pada Gambar 3.



Gambar 3 Persentase pengaduan per kategori Dwi Bulan IV 2014

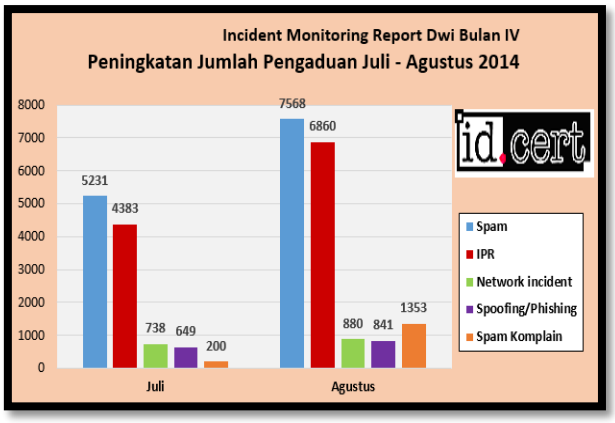
Untuk mengetahui perkembangan naik maupun turun dalam bentuk persentase dapat dilihat pada Tabel 2 berikut.

Kategori	JULI	AGUSTUS	%
Spam	5231	7568	44.68%
IPR	4383	6860	56.51%
Network incident	738	880	19.24%
Spoofing/Phishing	649	841	29.58%
Malware	414	173	-58.21%
Spam Komplain	200	1353	576.50%
Respon	179	154	-13.97%

Tabel 2 Perkembangan jumlah pengaduan dalam persentase

3.1 Kelompok pengaduan yang mengalami peningkatan

Ada beberapa kategori yang mengalami peningkatan jumlah pengaduan pada Juli – Agustus yaitu, *Spam* dari 5231 pada Juli menjadi 7568 di Agustus mengalami peningkatan 44,68%, IPR dari 4383 pada Juli menjadi 6860 di Agustus mengalami peningkatan 56,51%, *Network incident* dari 738 pada Juli menjadi 880 di Agustus mengalami peningkatan 19,24%, *Spoofing/phishing* dari 649 pada Juli menjadi 841 di Agustus mengalami peningkatan 29,58%, dan *Spam* komplain dari 200 di Juli menjadi 1353 di Agustus mengalami peningkatan 576,50% seperti di sajikan pada Gambar 4 di bawah.

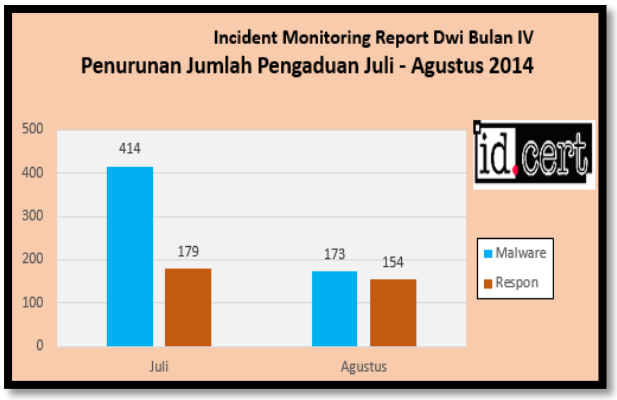


Gambar 4 Peningkatan jumlah pengaduan dari Juli – Agustus 2014

3.2 Kelompok pengaduan yang mengalami penurunan

Dari sekian banyak kategori pengaduan terdapat dua kategori yang mengalami penurunan jumlah pengaduan yaitu:

Malware yang mempunyai jumlah pengaduan sebesar 414 di Juli turun menjadi 173 di Agustus mengalami penurunan sebesar 58,21%. Kemudian, respon juga mengalami penurunan sebesar 13,97% dari 179 pada bulan Juli turun menjadi 154 di bulan Agustus. Disajikan pada Gambar 4 berikut.



Gambar 5 Penurunan Jumlah Pengaduan pada bulan Juli – Agustus 2014

Jika dilihat dari pesan pengaduan yang diterima, pengaduan ini diterima dari pelaporan non-otomatis, yakni pengaduan yang dikirim oleh pengguna komputer (bukan dari perangkat lunak atau alat bantu).

Dari beberapa kemungkinan akan fenomena di atas, dua hal perlu dipertimbangkan:

1. Pengguna Internet "menyelesaikan sendiri" urusan *spam*, baik menggunakan fasilitas pelaporan yang sudah disediakan layanan (sebagai misal hampir semua layanan email berbasis *web* sudah menyediakan penandaan "pesan sebagai *spam*") atau membiarkan *spam* ini dengan cukup menghapusnya.
2. ID-CERT perlu terus merangkul pihak-pihak lain untuk sosialisasi mekanisme pengaduan agar dapat menjaring lebih banyak laporan.

4. Rangkuman

Dengan pertimbangan jumlah pengaduan *spam* masih tertinggi, perlu menjadi perhatian para administrator jaringan, baik untuk jaringan lokal atau jaringan di bawah layanan Penyedia Jasa Internet (PJI), agar mempertimbangkan tindakan preventif mengurangi "pintu gerbang" pengiriman *spam* (terutama lewat email) dan mengantisipasi kedatangan *spam*.

Pada bulan Juli dan Agustus ini, jumlah pengaduan *spam* sangat dominan dibanding kategori lainnya meskipun terjadi penurunan pada bulan kedua.

Dilihat dari volume pengaduan yang masuk, yang menggambarkan kepedulian para pelapor terhadap isu keamanan Internet menjadi tanggung jawab pihak-pihak terkait dengan bahan laporan tersebut untuk menindaklanjuti dalam bentuk respon atau aksi yang diperlukan. Dengan demikian prosedur standar yang menjadi acuan dapat dijalankan dengan baik dan kepercayaan pihak pelapor terjaga atau meningkat.

4.1 Rekomendasi

Sejumlah rekomendasi yang dapat dipertimbangkan:

1. Perangkat lunak anti-*spam* dipasang di server email sebagai antisipasi pengiriman pesan *spam* dari jaringan lokal ke Internet.
2. Perangkat lunak anti virus dan perangkat lunak keamanan dipasang untuk mengurangi risiko terinfeksi *malware*. Pemutakhiran terhadap aplikasi dan basis data yang terkait dengan aplikasi dilakukan secara teratur.
3. Administrator jaringan perlu melakukan pemantauan terhadap aksi yang mencurigakan, misalnya akses ke port

email/Postfix[6] secara intensif dalam periode lama atau berulang-ulang.
4. Administrator jaringan memblokir semua port akses ke Internet, kecuali untuk port yang dianggap diperlukan.
5. Penyedia Jasa Internet (PJI/ISP) dan operator telekomunikasi disarankan menyediakan tombol pelaporan khusus penyalahgunaan Internet (*Internet abuse*) guna kemudahan pelaporan.
6. Formulir pengaduan penyalahgunaan Internet (*Internet abuse*) dicantumkan di setiap situs web.
7. Terkait Hak atas Kekayaan Intelektual (HaKI), sebaiknya pemerintah menyiapkan aturan hukum yang jelas mengenai materi (*content*) yang dianggap melanggar HaKI, karena PJI atau penyedia materi memerlukan landasan hukum yang jelas untuk menurunkan materi yang bermasalah.

Semua pihak wajib menindaklanjuti setiap laporan keluhan/pengaduan yang diterimanya. Bila menyangkut pelanggaran hukum, sebaiknya dilaporkan kepada penegak hukum.

5. Ucapan Terima Kasih

Laporan ini bisa disajikan karena adanya partisipasi dari beberapa pihak dalam hal pengumpulan bahan untuk penulisan laporan ID-CERT, yakni:

1. Kementrian Komunikasi dan Informatika (Kominfo)
2. Pengelola Nama Domain Internet Indonesia (PANDI)
3. Asosiasi Penyelenggaraan Jasa Internet Indonesia (APJII)
4. Detik (detik.net)
5. Tiga operator telekomunikasi, tujuh NAP, dan dua puluh dua PJI/ISP
6. Kemendikbud

[6] Postfix adalah perangkat lunak server email atau dikenal dengan Mail Transfer Agent (MTA) dan berdasarkan perhitungan tahun 2012 disebut digunakan oleh 23% server email di Internet.

Sumber: Wikipedia, http://en.wikipedia.org/wiki/Postfix_(software)