Laporan Dwi Bulan III 2014

Mei - Juni 2014

ID-CERT[1]

Ringkasan

Di Laporan Dwi Bulan III 2014 ini disajikan hasil pengumpulan pengaduan selama dua bulan yaitu Mei dan Juni 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/phising, 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 antar warga 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. Seiring dengan perkembangan yang demikian pesatnya terutama penyalah gunaan dan kejahatan melalui internet maka aspek keamanan Internet (*Internet security*) juga menjadi sisi yang perlu secara khusus menjadi perhatian dan kerja sama banyak kalangan.
Sebagai bagian dari pemantauan keamanan Internet, ID-CERT[1] juga telah mengadakan kerjasama dengan beberapa pihak serta menerima pengaduan lewat e-mail yang diterima dari beberapa responden. Dari pengaduan yang masuk tersebut dilakukan pengelompokan dalam sejumlah kategori dan disajikan dalam bentuk laporan Dwi Bulan. Laporan ini sebagai paparan gambaran insiden keamanan (*security incident*) yang terjadi selama dua bulan, Mei dan Juni 2014.

[1] Indonesian Computer Emergency Respons 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 penyalah gunaan 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 III 2014 ini spam masih menempati jumlah pengaduan terbanyak yaitu mencapai 60,00%, jumlah tersebut lebih tiga kalinya dari IPR yang menempati urutan pengaduan ke dua yaitu sebesar 15,78%. Dilihat dari sisi jumlah pengaduan, terdapat tiga kelompok besar: spam sendiri pada kelompok pertama yang mencapai jumlah di atas 10.000 pengaduan, dikuti kelompok ke dua yang memiliki jumlah pelaporan sedang yaitu di bawah 10.000 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 e-mail 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 dan dikelompok-kan oleh responden.

Dari laporan yang sudah terkumpul, dilakukan pengelompokan dalam beberapa kategori 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 e-mail 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.

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.

---

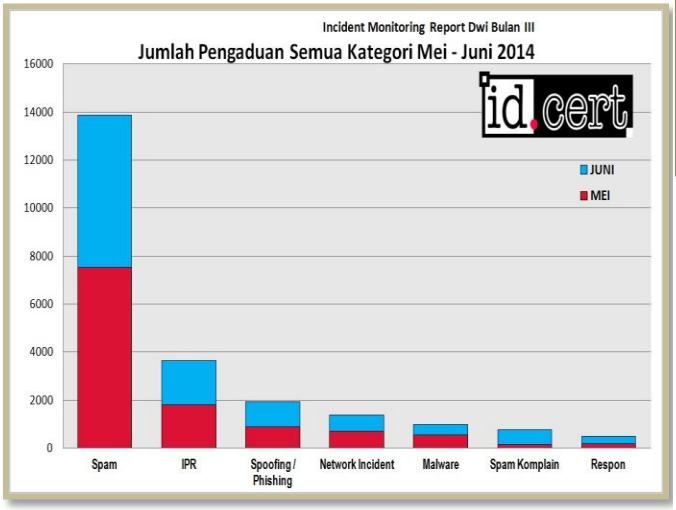
[2] ***Fraud,*** http://en.wikipedia.org/wiki/Fraud
[3] ***Malware,*** http://en.wikipedia.org/wiki/Malware
[4] ***Spam(electronic),***http://en.wikipedia.org/wiki/Spam_(electronic)
[5] ***Spoofing attack,*** http://en.wikipedia.org/wiki/Spoofing_attack

3. Uraian

Email pengaduan yang diterima dikumpulkan berdasarkan kategori pengaduan dan bulan penerimaan laporan, dengan demikian terdapat dua kelompok besar, bulan Mei dan Juni 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 terformat bagus, karena email 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 III 2014 berdasarkan jumlah pengaduan per bulan ditampilkan pada Gambar 1.



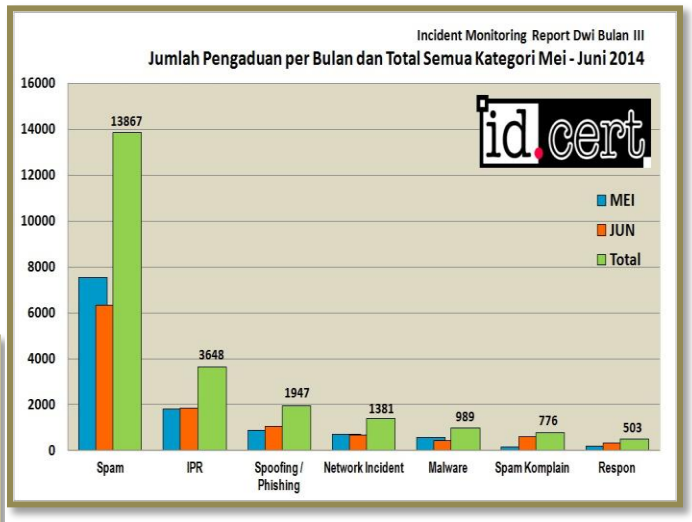
Gambar 1. Jumlah pengaduan semua kategori Mei - Juni 2014

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 Mei - Juni 2014

Kategori	MEI	JUNI	Total	%
Spam	7,535	6,332	13,867	60.00%
IPR	1,816	1,832	3,648	15.78%
Spoofing / Phishing	883	1,064	1,947	8.42%
Network Incident	711	670	1,381	5.98%
Malware	575	414	989	4.28%
Spam Komplain	165	611	776	3.36%
Respon	187	316	503	2.18%

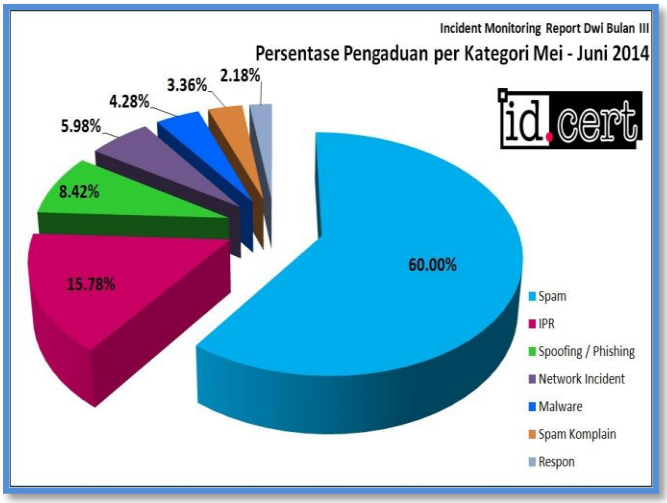
Pada Gambar 2 bisa dilihat perkembangan dari naik atau turunnya jumlah pengaduan antara bulan Mei dan Juni 2014 dan jumlah total dua bulan.



Gambar 2. Jumlah pengaduan per bulan dan total semua kategori Mei - Juni 2014.

Perhitungan perkembangan dilakukan terhadap jumlah pengaduan pada bulan pertama Mei, bulan kedua Juni dan bernilai negatif jika terjadi penurunan. Secara umum tidak ada tren yang terjadi dari jumlah pengaduan Mei di banding Juni karena masing-masing kategori ada yang meningkat yaitu *IPR*, *Spoofing/phising*, *Spam* Komplain tetapi ada pula yang menurun yaitu

Spam, *Malware*. Meskipun Spam terjadi penurunan jumlah pengaduan tetapi masih menempati urutan pertama dalam jumlah pengaduan yaitu mencapai 60% dari total pengaduan di bulan Mei dan Juni, persentase detail dari masing-masing dihitung terhadap jumlah pengaduan keseluruhan dapat dilihat pada Tabel 1. Tampilan tabel tersebut berdasarkan urutan persentase kategori dari terbanyak. Untuk melihat perbandingan besar persentase jumlah laporan antar semua kategori ditampilkan dalam bentuk diagram lingkaran yang disajikan pada Gambar 2.



Gambar 2. Persentase pengaduan per kategori Dwi Bulan II 2014.

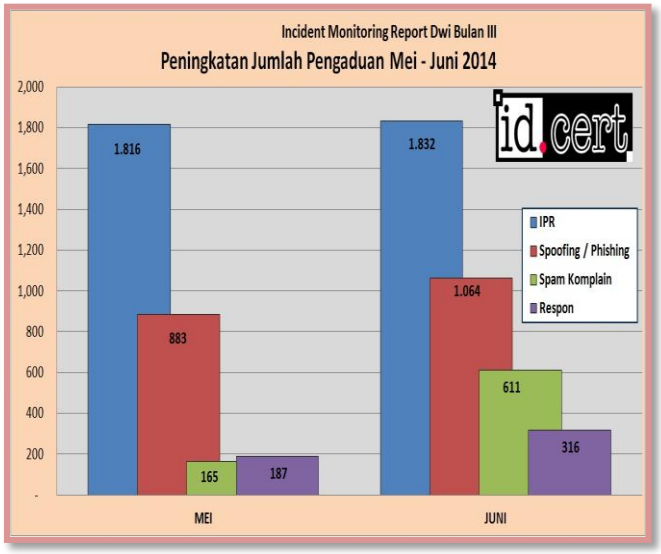
Untuk mengetahui perkembangan naik maupun turun dalam bentuk persentase dapat dilihat pada Tabel 2 berikut.

Tabel 2. Perkembangan jumlah pengaduan dalam persentase.

Kategori	MEI	JUNI	%
Spam	7,535	6,332	-19.00%
IPR	1,816	1,832	0.87%
Spoofing / Phishing	883	1,064	17.01%
Network Incident	711	670	-6.12%
Malware	575	414	-38.89%
Spam Komplain	165	611	73.00%
Respon	187	316	40.82%

3.1. Kelompok pengaduan yang mengalami peningkatan.

Ada beberapa kategori yang mengalami peningkatan jumlah pengaduan pada Mei – Juni yaitu :
IPR dari 1.816 pada Mei menjadi 1.832 di Juni mengalami peningkatan 0,87 %, *Spoofing/ phising* dari 883 pada Mei menjadi 1.064 di Juni mengalami peningkatan 17,01 %, spam komplain dari 165 di Mei menjadi 611 di Juni mengalami peningkatan 73,00 %, dan respon dari 187 di Mei menjadi 316 di Juni terjadi peningkatan 40,82 % seperti di sajikan pada Gambar 3 di bawah.

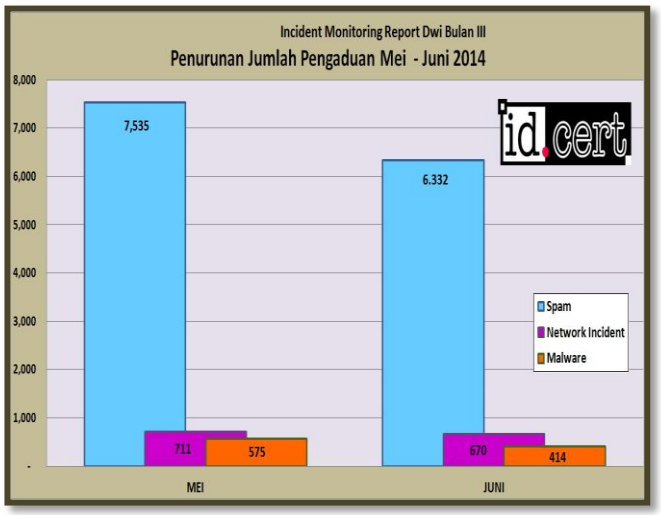


Gambar 3. Peningkatan jumlah pengaduan dari Mei – Juni 2014.

3.2. Kelompok pengaduan yang mengalami penurunan.

Dari sekian banyak kategori pengaduan terdapat tiga kategori yang mengalami penurunan jumlah pengaduan yaitu :
Spam yang mempunyai jumlah pengaduan sebesar 7.535 di Mei turun menjadi 6.332 di Juni mengalami penurunan sebesar 19,00 %, *network incident* adalah kategori kedua yang mengalami penurunan dari 711 di bulan Mei menjadi 670 di bulan Juni terjadi penurunan sebesar 6,12 % dan kategori terakhir adalah *malware* dengan jumlah 575 di bulan Mei turun menjadi 414 di bulan

Juni yang artinya sama dengan penurunan sebesar 38,89 %. Disajikan pada Gambar 4 berikut.



Gambar 4. Penurunan Jumlah Pengaduan pada bulan Mei – Juni 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 semualayanan 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*.
Dua bulan kedua ini, Mei dan Juni, 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. Perangakat lunak anti-spam dipasang di server email sebagai antisipasi pengiriman pesan spam dari jaringan lokan ke Internet.
2. Perangakat lunak anti virus dan perangkat lunak keamanan dipasang untuk mengu-rangi resiko terinfeksi malware. Pemutakhiran terhadap aplikasi dan basis data yang terkait dengan aplikasi dilakukan secara tertatur.
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.

[6] **Posfix** 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)

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

KEMENDIKBUD