Incident Monitoring Report - 2015

Laporan Dwi Bulanan I 2015

Bulan Januari dan Februari 2015

Februari 2015

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 penyalahgunaan 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 email 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, Januari dan Februari 2015.

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 I 2015 ini, *spam* masih menempati jumlah pengaduan terbanyak yaitu mencapai 30,99%, sedangkan Respon menempati urutan pengaduan kedua dengan selisih sekitar 3% dari *spam* yaitu sebesar 27,31%. Dilihat dari sisi jumlah pengaduan, terdapat dua kelompok besar: *spam* pada kelompok pertama 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.

[1] Indonesian Computer Emergency Response Team

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 dan dikelompokkan 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 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.

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.

---

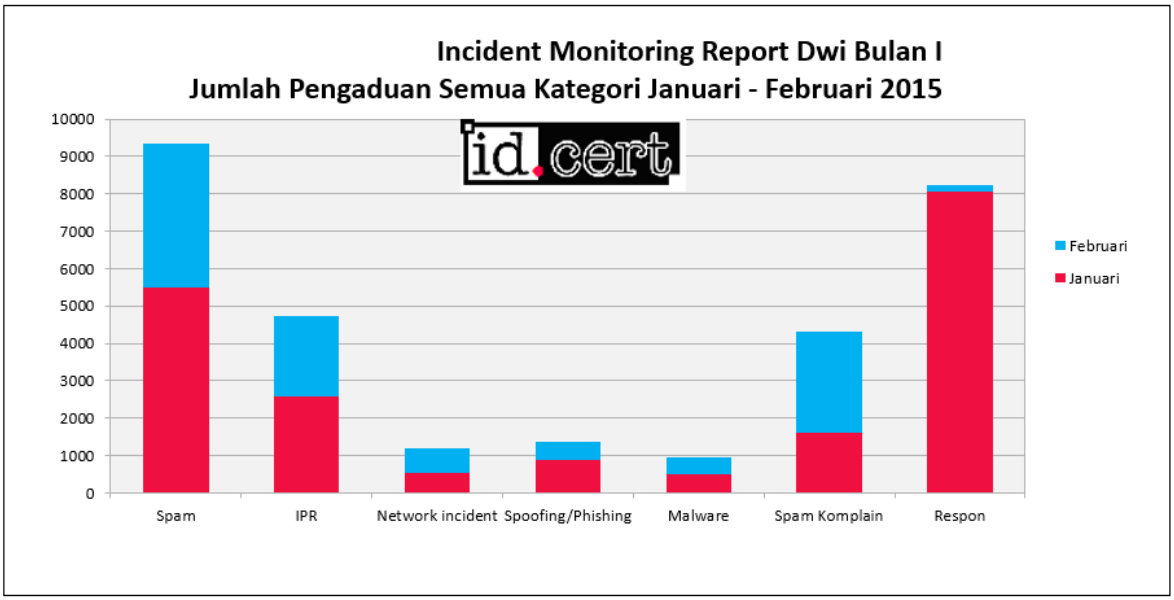
[2] *Fraud*, `http://en.wikipedia.org/wiki/Fraud`
[3] *Malware*, `http://en.wikipedia.org/wiki/Malware`
[4] *Spam (electronic)*, `http://en.wikipedia.org/wiki/Spam_(electronic)`
[5] *Spoofing attack*, `http://en.wikipedia.org/wiki/Spoofing_attack`

3. Uraian

Email pengaduan yang diterima dikumpulkan berdasarkan kategori pengaduan dan bulan penerimaan laporan, dengan demikian terdapat dua kelompok besar, bulan Januari dan Februari 2015. 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 I 2015 berdasarkan jumlah pengaduan per bulan ditampilkan pada Gambar 1.



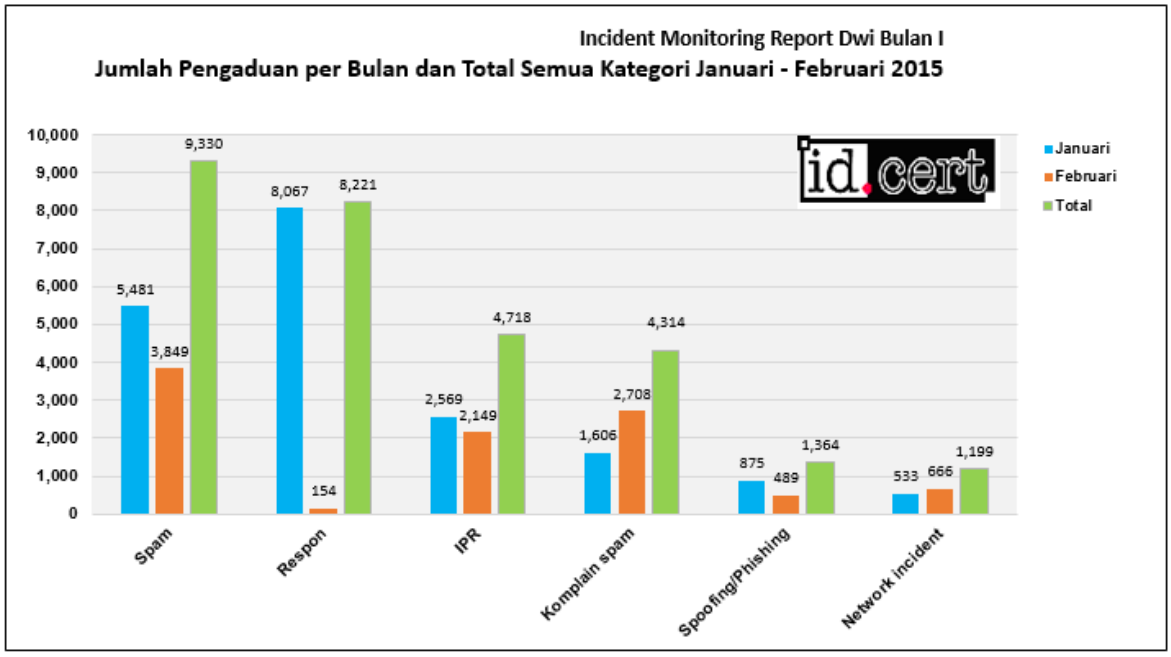
Gambar 1. Jumlah pengaduan semua kategori Januari - Februari 2015

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 tertinggi ke terendah.

Tabel 1. Perkembangan jenis pengaduan selama Januari - Februari 2015

Kategori	Januari	Februari	Total	%
Spam	5,481	3,849	9,330	30.99%
Respon	8,067	154	8,221	27.31%
IPR	2,569	2,149	4,718	15.67%
Komplain spam	1,606	2,708	4,314	14.33%
Spoofing/Phishing	875	489	1,364	4.53%
Network incident	533	666	1,199	3.98%
Malware	486	470	956	3.18%

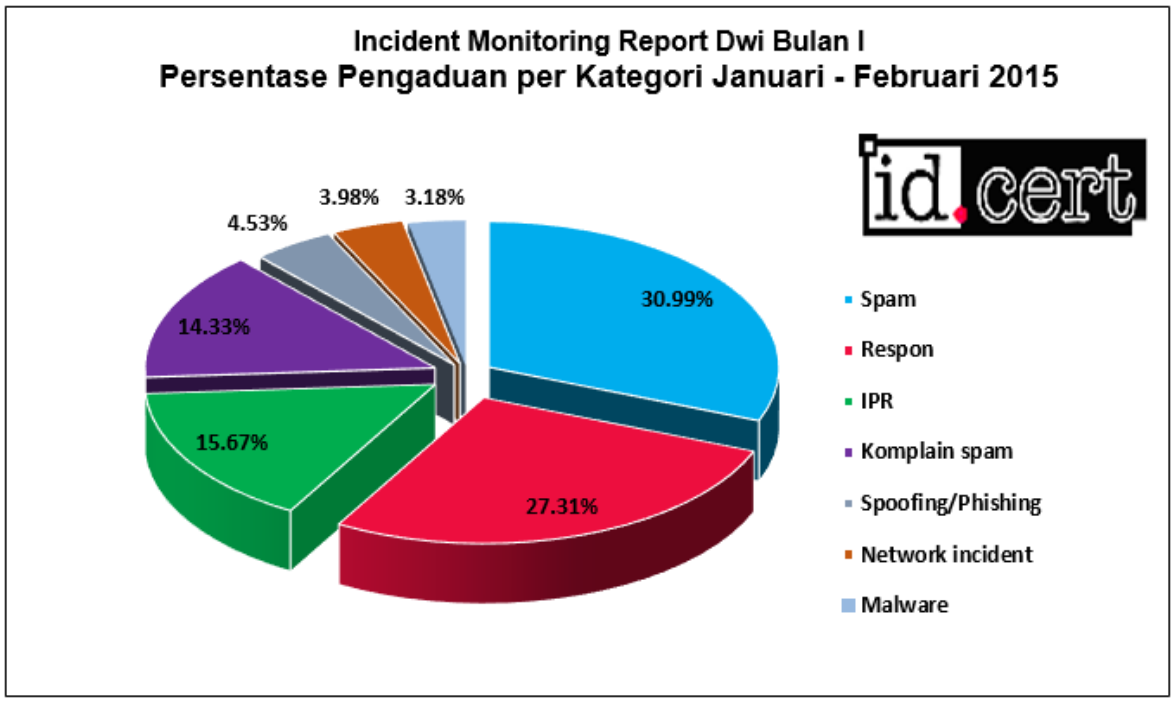
Pada Gambar 2 dapat dilihat perkembangan dari naik atau turunnya jumlah pengaduan antara bulan Januari - Februari 2015 dan jumlah total dua bulan.



Gambar 2. Jumlah pengaduan per bulan dan total semua kategori Januari - Februari 2015

Perhitungan perkembangan dilakukan terhadap jumlah pengaduan pada bulan pertama Januari, bulan kedua Februari dan bernilai negatif jika terjadi penurunan. Secara umum tidak ada tren yang terjadi dari jumlah pengaduan Januari di banding Februari karena masing-masing kategori ada yang meningkat yaitu Network Incident dan Spam Komplain tetapi ada pula yang menurun yaitu Spam,

IPR, Malware, Spoofing/Phishing, Respon. 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 2015

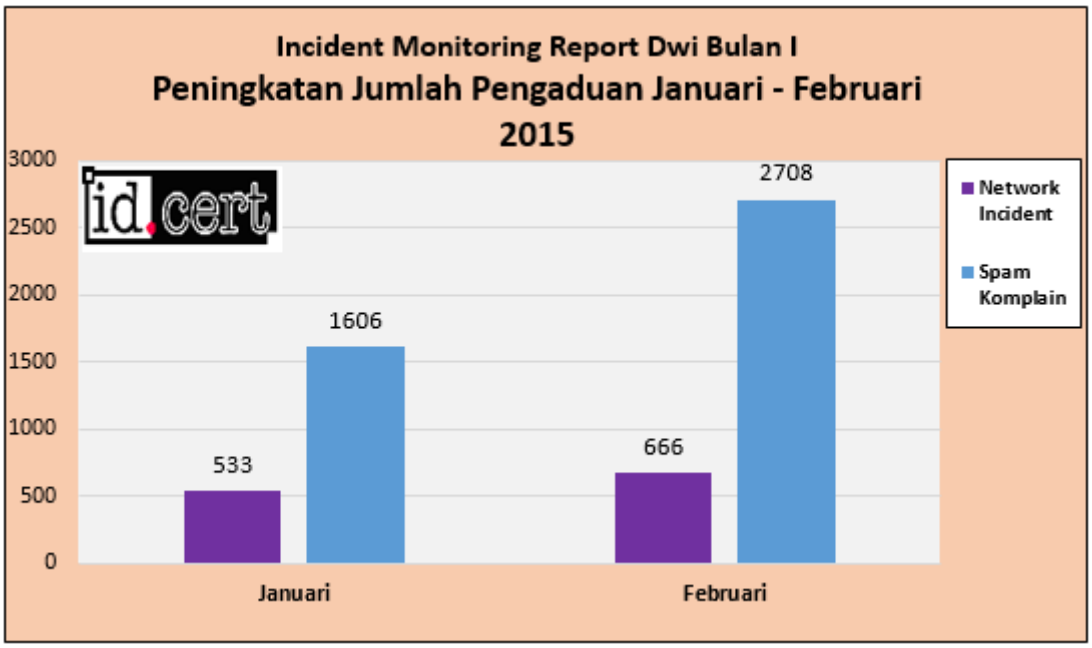
Untuk mengetahui perkembangan naik maupun turun dalam bentuk persentase dapat dilihat pada Tabel 2 berikut.

Kategori	Januari	Februari	%
Respon	8067	154	-98.09%
Spoofing/Phishing	875	489	-44.11%
Spam	5481	3849	-29.78%
IPR	2569	2149	-16.35%
Malware	486	470	-3.29%
Network incident	533	666	24.95%
Spam Komplain	1606	2708	68.62%

Tabel 2. Perkembangan jumlah pengaduan dalam persentase

3.1. Kelompok pengaduan yang mengalami peningkatan.

Pada bulan Januari – Februari, ada kategori yang mengalami peningkatan jumlah pangaduan, yaitu Network Incident dan Spam Komplain. Jumlah Network Incident pada bulan Januari sebesar 533, mengalami peningkatan pada bulan Februari menjadi 666. Persentase peningkatan jumlah pengaduan Network Incident yaitu 24.95%. Jumlah spam komplain pada bulan Januari sebesar 1.606, mengalami peningkatan pada bulan Februari menjadi 2.708. Persentase peningkatan jumlah pengaduan spam komplain yaitu 68.62%. Grafik peningkatan jumlah pengaduan bulan Januari – Februari disajikan pada Gambar 4.



Gambar 4. Peningkatan jumlah pengaduan dari Januari – Februari 2015

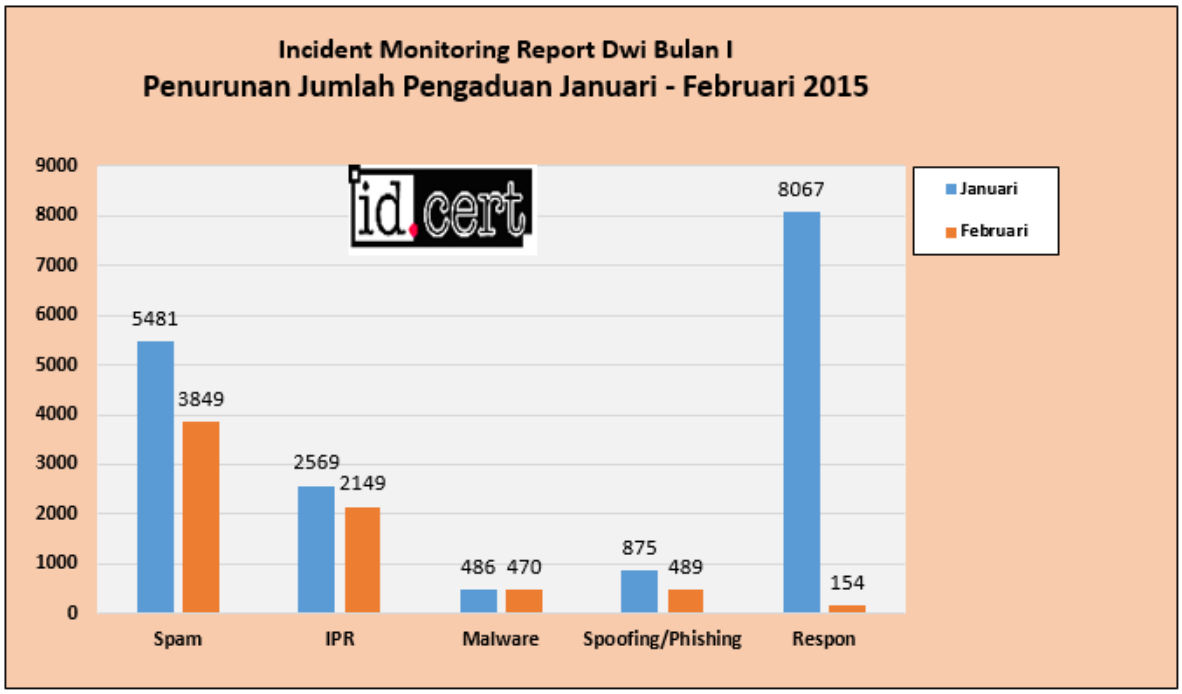
3.2. Kelompok pengaduan yang mengalami penurunan.

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

1. Respon mempunyai jumlah pengaduan sebesar 8.067 di bulan Januari, turun menjadi 154 pada Februari dengan persentase penurunan sebesar 98.09%.
2. Spoofing/Phising mempunyai jumlah pengaduan sebesar 875 di bulan Januari, turun menjadi 489 di Februari dengan persentasi penurunan sebesar 44,11%.
3. Spam mempunyai jumlah pengaduan sebesar 5.481 di bulan Januari, turun menjadi 3.849 di Februari dengan persentase penurunan sebesar 29,78%.

4. IPR mempunyai jumlah pengaduan sebesar 2.569 di bulan Januari, turun menjadi 2.149 di Februari dengan persentase penurunan sebesar 16,35%.
5. Malware mempunyai jumlah pengaduan sebesar 486 di bulan Januari, turun menjadi 470 di Februari dengan persentase penurunan sebesar 3,29%.

Grafik penurunan pengaduan tersebut disajikan pada Gambar 5.



Gambar 5. Penurunan Jumlah Pengaduan pada bulan Januari – Februari 2015

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.

Dua bulan kedua ini, Januari dan Februari, jumlah pengaduan spam sangat dominan dibanding kategori lainnya dan terjadi peningkatan 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 antivirus dan perangkat lunak keamanan dipasang untuk mengurangi risiko 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.
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