Laporan Dwi Bulanan III 2017

Bulan Mei dan Juni 2017

Juli 2017

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 lanjut usia, 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 Bulanan. Laporan ini sebagai paparan gambaran insiden keamanan (*security incident*) yang terjadi selama dua bulan, Mei dan Juni 2017.

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.

1 Indonesia Computer Emergency Response Team

Pada laporan Dwi Bulanan III 2017 ini, *Spam* menempati jumlah pengaduan terbanyak yaitu mencapai 37,51% atau berjumlah total 5.613 aduan. Dilihat dari sisi jumlah pengaduan, terdapat dua kelompok: *Spam, Network Incident,* Komplain Spam, *Malware*, *Spoofing/Phishing*, dan HaKI/IPR pada kelompok pertama yang memiliki jumlah pelaporan di atas 1.000 laporan, dan hanya satu yaitu Respon pada kelompok kedua yang berjumlah pengaduan rendah yaitu di bawah 1.000 pengaduan. Penjelasan lengkap tentang kedua kelompok tersebut dipaparkan di bagian Uraian.

Pembuatan laporan ini berdasarkan pada data-data yang diperoleh dan diambil dari 41 (empat puluh satu) responden yang diantaranya terdiri dari: Kominfo, ID-CERT, PANDI, APJII, Detik.net, Zone-h, Anti Fraud Command Center (AFCC), dan Kaspersky, 3 (tiga) operator telekomunikasi, 7 (tujuh) NAP, 22 (dua puluh dua) Penyedia Jasa Internet (PJI/ISP), dan KEMDIKBUD.

2. Metoda

Penyusunan dokumen Dwi Bulanan III 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 menjadi kategori berikut ini:

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.

4 *Spam (electronic)*, http://en.wikipedia.org/wiki/Spam_(electronic)
5 *Spoofing attack*, http://en.wikipedia.org/wiki/Spoofing_attack

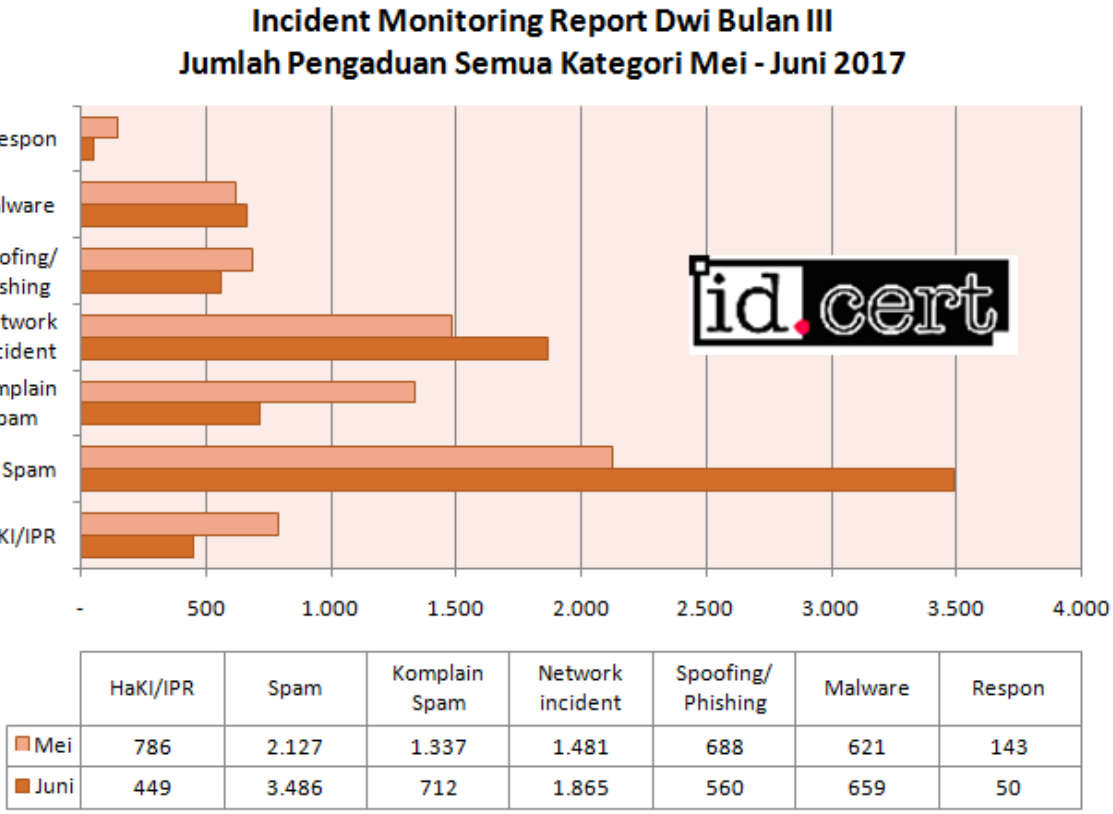
3. Uraian

Email pengaduan yang diterima dikumpulkan berdasarkan kategori pengaduan dan bulan, dengan demikian terdapat dua kelompok besar, yaitu bulan Mei dan Juni 2017. Kategori pengaduan terdiri atas *Spam, Network Incident,* Komplain *Spam*, *Malware, Spoofing/Phishing*, HaKI/IPR (Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR)), dan Respon.

Pengolahan data dilakukan dengan dua cara, yaitu:

1. Penghitungan jumlah dari *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 jumlah dari isi (*body*) email. 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 Bulanan III 2017 berdasarkan jumlah pengaduan per bulan ditampilkan pada Gambar 1 di bawah ini.



	HaKI/IPR	Spam	Komplain Spam	Network incident	Spoofing/ Phishing	Malware	Respon
Mei	786	2.127	1.337	1.481	688	621	143
Juni	449	3.486	712	1.865	560	659	50

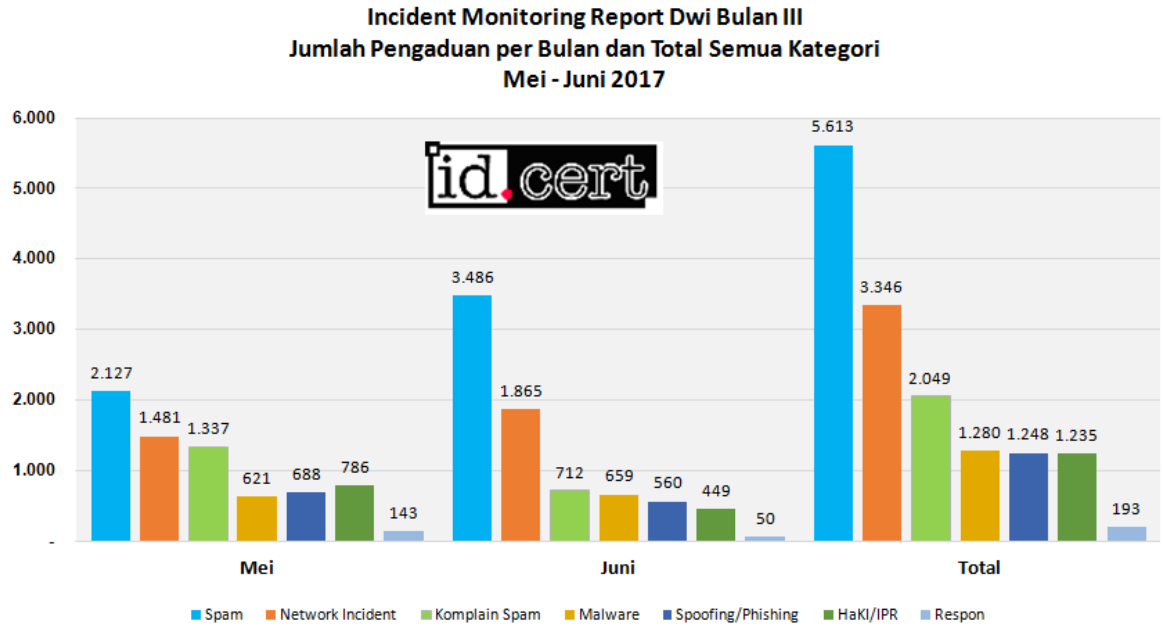
Gambar 1 Jumlah pengaduan semua kategori Mei – Juni 2017

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 Mei – Juni 2017

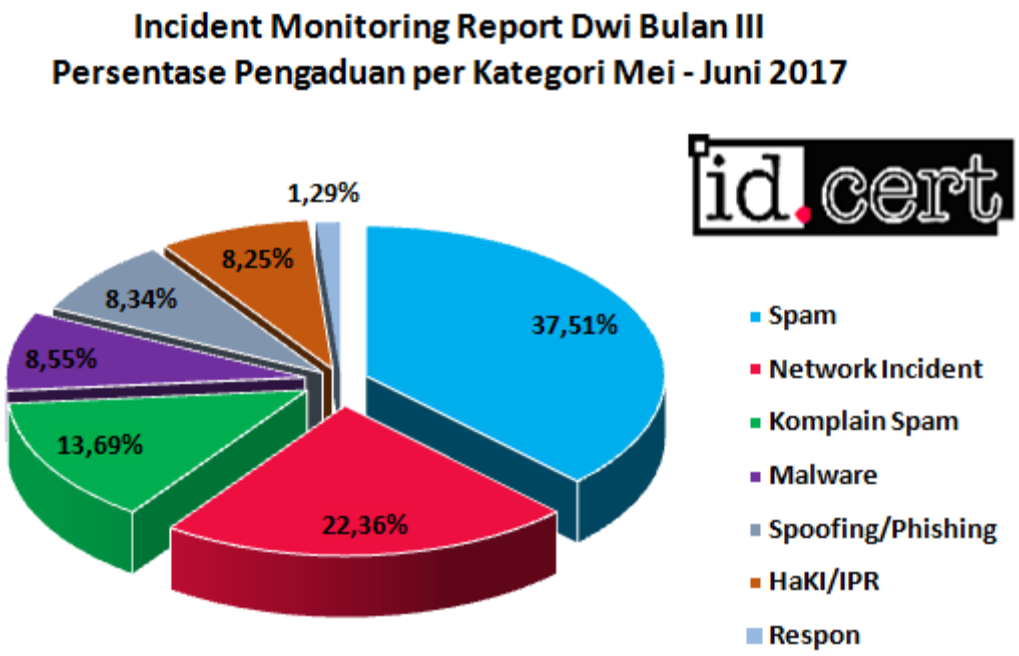
Kategori	Mei	Juni	Total	%
Spam	2.127	3.486	5.613	37,51%
Network Incident	1.481	1.865	3.346	22,36%
Komplain Spam	1.337	712	2.049	13,69%
Malware	621	659	1.280	8,55%
Spoofing/Phishing	688	560	1.248	8,34%
HaKI/IPR	786	449	1.235	8,25%
Respon	143	50	193	1,29%

Pada Gambar 2 dapat dilihat perkembangan ataupun penurunan dari jumlah pengaduan antara bulan Mei – Juni 2017 dan jumlah total dua bulan.



Gambar 2 Jumlah pengaduan per bulan dan total semua kategori Mei – Juni 2017

Perhitungan perkembangan dilakukan terhadap jumlah pengaduan pada bulan pertama Mei, bulan kedua Juni dan bernilai negatif jika terjadi penurunan. Tren untuk Dwi Bulanan III ini yaitu sebagian kategori mengalami peningkatan dan sebagian kategori lain mengalami penurunan jumlah pengaduan pada bulan Juni. Persentase detil 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 Bulanan III 2017

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

Tabel 2 Perkembangan jumlah pengaduan yang mengalami peningkatan dan penurunan dalam persentase

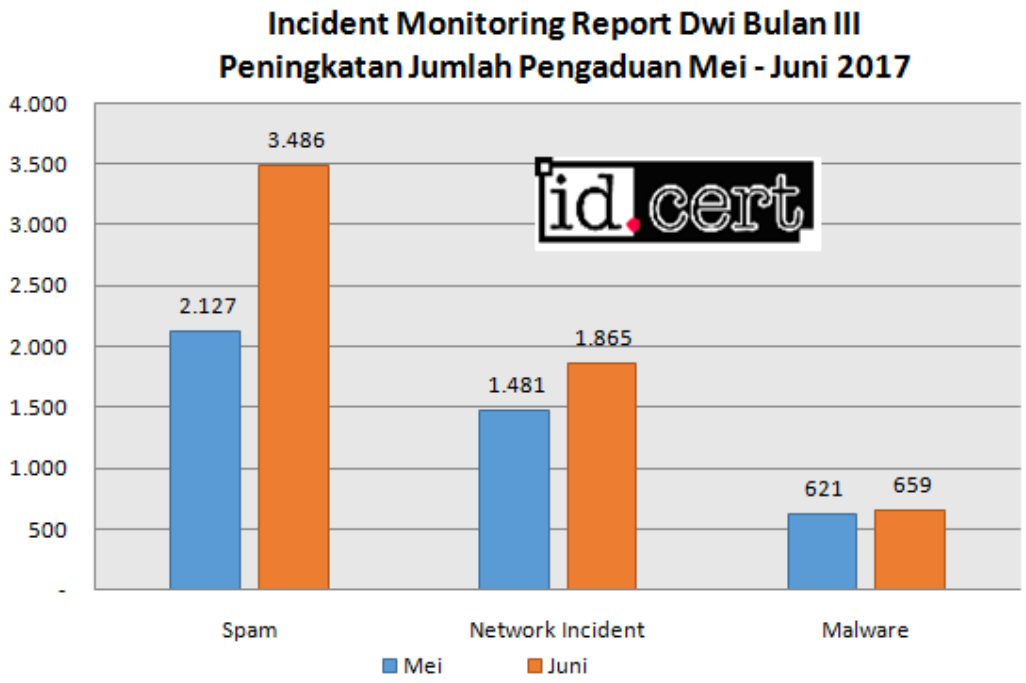
Kategori	Mei	Juni	%
Spam	2.127	3.486	63,89%
Network Incident	1.481	1.865	25,93%
Malware	621	659	6,12%
Spoofing/Phishing	688	560	-18,60%
HaKI/IPR	786	449	-42,88%
Komplain Spam	1.337	712	-46,75%
Respon	143	50	-65,03%

3.1 Kelompok Pengaduan yang Mengalami Peningkatan

Dari sekian banyak kategori pengaduan, terdapat 3 (tiga) kategori yang mengalami peningkatan jumlah pengaduan, yaitu:

1. *Spam* mengalami peningkatan jumlah pengaduan sebesar 1.359 dari bulan Mei ke Juni, dari 2.127 meningkat menjadi 3.486. Persentase peningkatannya mencapai sebesar 63,89%.
2. *Network Incident* jumlah pengaduannya meningkat 25,93% di bulan kedua. Di bulan pertama Mei jumlahnya sebesar 1.481 meningkat menjadi 1.865 pengaduan di bulan kedua Juni.
3. *Malware* juga mengalami sedikit peningkatan jumlah pengaduan, yaitu 38 atau 6,12% saja. Pada bulan Mei berjumlah 621 pengaduan, pada bulan Juni meningkat menjadi 659 pengaduan.

Grafik peningkatan pengaduan tersebut disajikan pada Gambar 4.



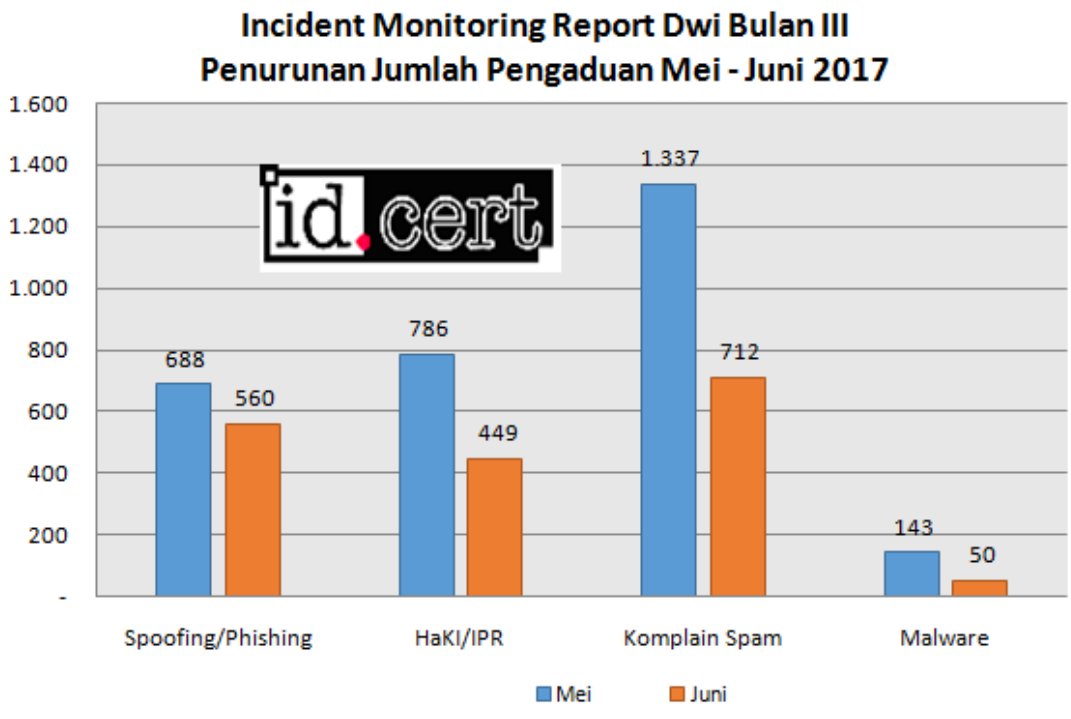
Gambar 4 Peningkatan Jumlah Pengaduan pada bulan Mei – Juni 2017

3.2 Kelompok Pengaduan yang Mengalami Penurunan

Bulan Mei – Juni 2017 terdapat beberapa kategori yang mengalami penurunan jumlah pengaduan di bulan kedua, yaitu:

1. *Spoofing/Phishing* mengalami penurunan jumlah pengaduan dari 688 pada bulan Mei dan turun sebesar 18,60% di bulan Juni dengan jumlah pengaduan sebanyak 560.
2. Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR) mengalami penurunan jumlah pengaduan dari bulan Mei ke Juni, dari 786 turun ke 449. Persentase penurunannya sebesar 42,88%.
3. Komplain *Spam* juga mengalami penurunan jumlah dari bulan Mei ke Juni ini. Komplain *Spam* memiliki jumlah sebanyak 1.337 pada bulan Mei dan turun dengan persentase sebesar 46,75% di bulan Juni dengan jumlah sebanyak 712.
4. Respon memiliki jumlah pengaduan sejumlah 143 di bulan Mei. Pada bulan Juni terjadi penurunan jumlah pengaduan dibandingkan dengan bulan Mei dengan persentase penurunan sebesar 65,03% yang berjumlah 50 pengaduan.

Grafik penurunan jumlah pengaduan disajikan pada Gambar 5.



Gambar 5 Penurunan Jumlah Pengaduan pada bulan Mei – Juni 2017

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* yang masih sangat tinggi, 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*.

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 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 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. KEMDIKBUD