

Laporan Dwi Bulanan II 2017

Bulan Maret dan April 2017



Mei 2017

Daftar Isi

1.Pendahuluan.....	3
2.Metoda.....	5
3.Uraian.....	7
3.1 Kelompok Pengaduan yang Mengalami Peningkatan.....	11
3.2 Kelompok Pengaduan yang Mengalami Penurunan.....	12
4.Rangkuman.....	14
4.1 Rekomendasi.....	14
5.Ucapan Terima Kasih.....	16

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-CERT¹ 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, Maret dan April 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 II 2017 ini, *Spam* menempati jumlah pengaduan terbanyak yaitu mencapai 48,74% atau berjumlah total 9.565 aduan. Dilihat dari sisi jumlah pengaduan, terdapat dua kelompok: *Spam*, *Network Incident*, Komplain Spam, HaKI/IPR, dan *Spoofing/Phishing* pada kelompok pertama yang memiliki jumlah pelaporan di atas 1.000 laporan, dan *Malware* dan Respon pada kelompok kedua 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 II 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 lain² 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 jahat³.

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-pilih⁴.

Spoofing/Phishing Pemalsuan email dan situs untuk menipu pengguna⁵.

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

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

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

3. Uraian

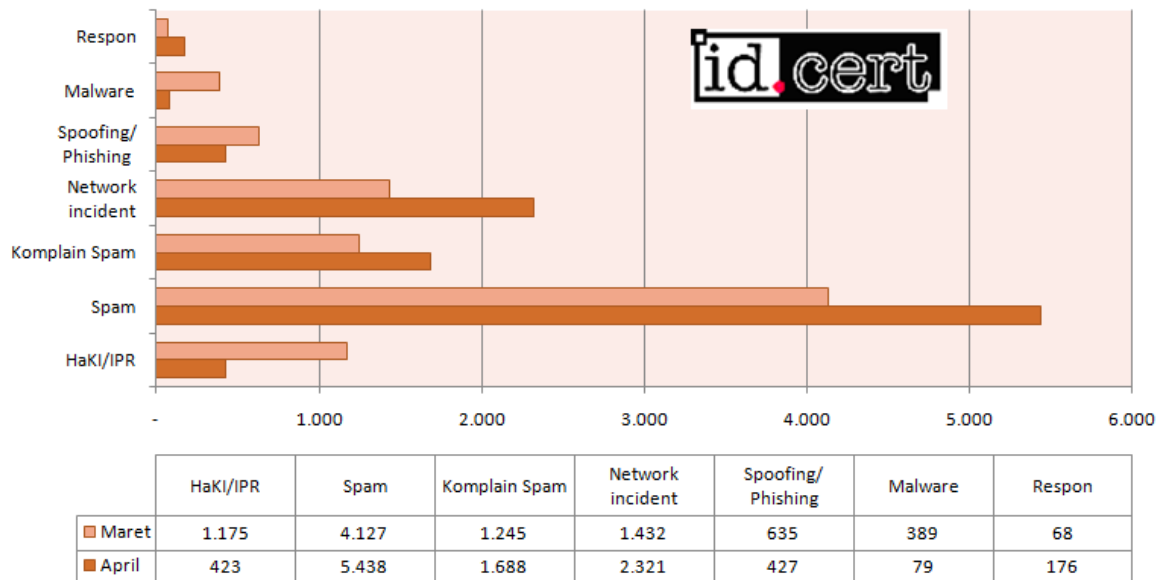
Email pengaduan yang diterima dikumpulkan berdasarkan kategori pengaduan dan bulan, dengan demikian terdapat dua kelompok besar, yaitu bulan Maret dan April 2017. Kategori pengaduan terdiri atas *Spam*, *Network Incident*, *Komplain Spam*, *HaKI/IPR* (Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR)), *Spoofing/Phishing*, *Malware*, 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 II 2017 berdasarkan jumlah pengaduan per bulan ditampilkan pada Gambar 1 di bawah ini.

Incident Monitoring Report Dwi Bulan II
Jumlah Pengaduan Semua Kategori Maret - April 2017



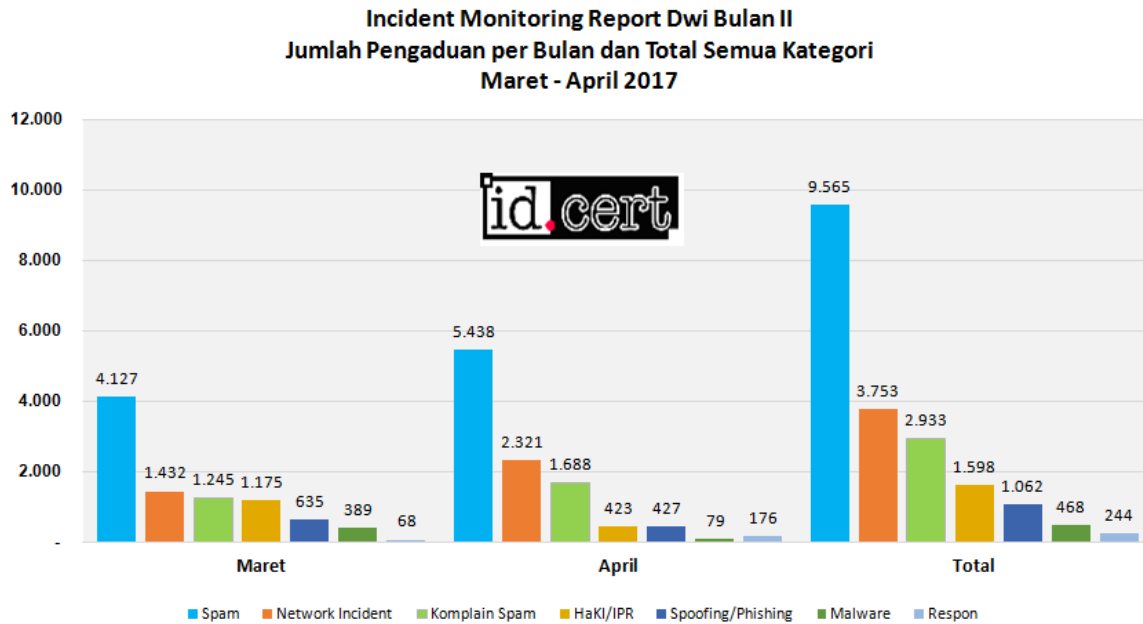
Gambar 1 Jumlah pengaduan semua kategori Maret – April 2017

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 Maret – April 2017

Kategori	Maret	April	Total	%
Spam	4.127	5.438	9565	48,74%
Network Incident	1.432	2.321	3753	19,13%
Komplain Spam	1.245	1.688	2933	14,95%
HaKI/IPR	1.175	423	1598	8,14%
Spoofing/Phishing	635	427	1062	5,41%
Malware	389	79	468	2,38%
Respon	68	176	244	1,24%

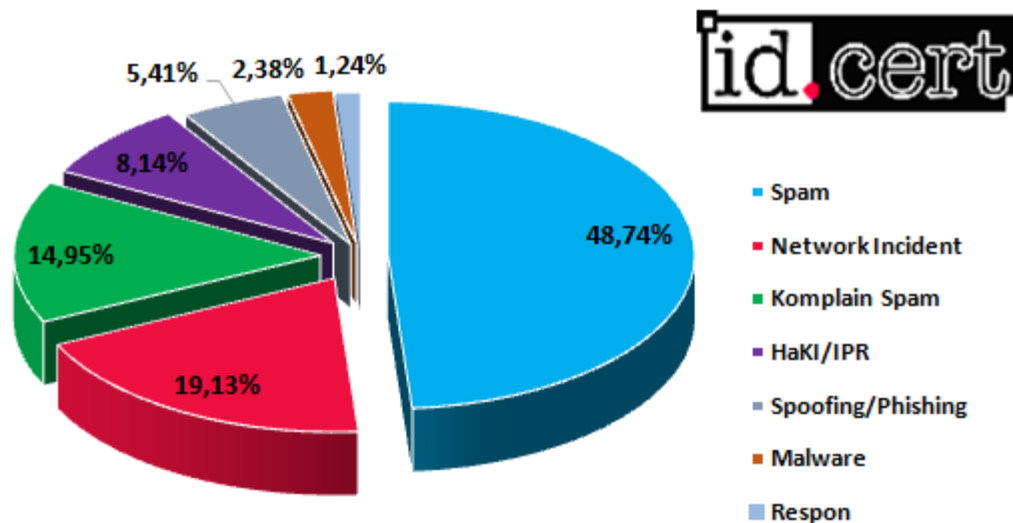
Pada Gambar 2 dapat dilihat perkembangan ataupun penurunan dari jumlah pengaduan antara bulan Maret – April 2017 dan jumlah total dua bulan.



Gambar 2 Jumlah pengaduan per bulan dan total semua kategori Maret – April 2017

Perhitungan perkembangan dilakukan terhadap jumlah pengaduan pada bulan pertama Maret, bulan kedua April dan bernilai negatif jika terjadi penurunan. Tren untuk Dwi Bulanan II ini yaitu sebagian kategori yang mengalami peningkatan dan sebagian kategori lain mengalami penurunan jumlah pengaduan pada bulan April. 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.

Incident Monitoring Report Dwi Bulan II Persentase Pengaduan per Kategori Maret - April 2017



Gambar 3 Persentase pengaduan per kategori Dwi Bulanan II 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

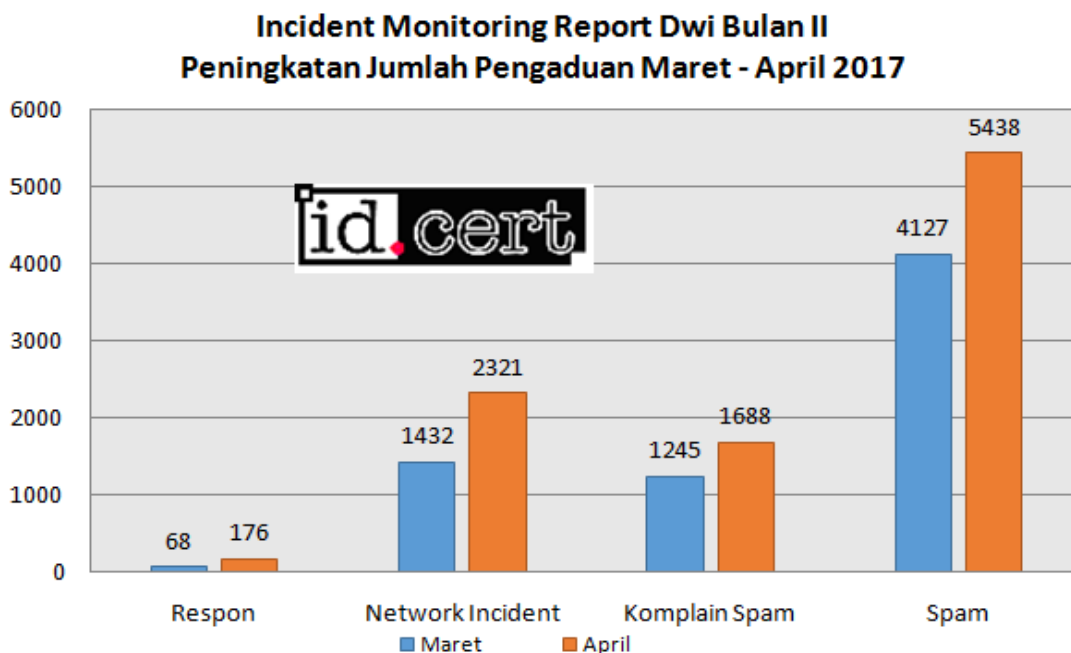
Kategori	Maret	April	%
Respon	68	176	158,82%
Network Incident	1.432	2.321	62,08%
Komplain Spam	1.245	1.688	35,58%
Spam	4.127	5.438	31,77%
Spoofing/ Phishing	635	427	-32,76%
HaKI/IPR	1.175	423	-64,00%
Malware	389	79	-79,69%

3.1 Kelompok Pengaduan yang Mengalami Peningkatan

Selama bulan Maret dan April 2017 terdapat 4 (empat) kategori yang mengalami peningkatan jumlah pengaduan, yaitu:

1. Respon mengalami peningkatan jumlah dari bulan Maret ke April, dari 68 meningkat menjadi 176, dan bila dipersentasekan peningkatannya mencapai sebesar 158,82%.
2. *Network Incident* peningkatan jumlah aduannya mencapai 62,08%, yaitu dari 1.432 aduan di bulan Maret meningkat menjadi 2.321 di bulan April.
3. *Komplain Spam* juga mengalami peningkatan jumlah aduan sebesar 443 aduan, di bulan Maret sebesar 1.245 menjadi 1.688 di bulan April, dengan persentase peningkatan sebesar 35,58%.
4. *Spam* bila dilihat dari angka memang banyak jumlah aduannya, yaitu 4.127 aduan di bulan Maret meningkat menjadi 5.438 aduan di bulan April, tetapi persentase peningkatannya paling kecil di antara kategori lainnya yang mengalami peningkatan jumlah aduan, yaitu sebesar 31,77%.

Grafik peningkatan pengaduan tersebut disajikan pada Gambar 4.



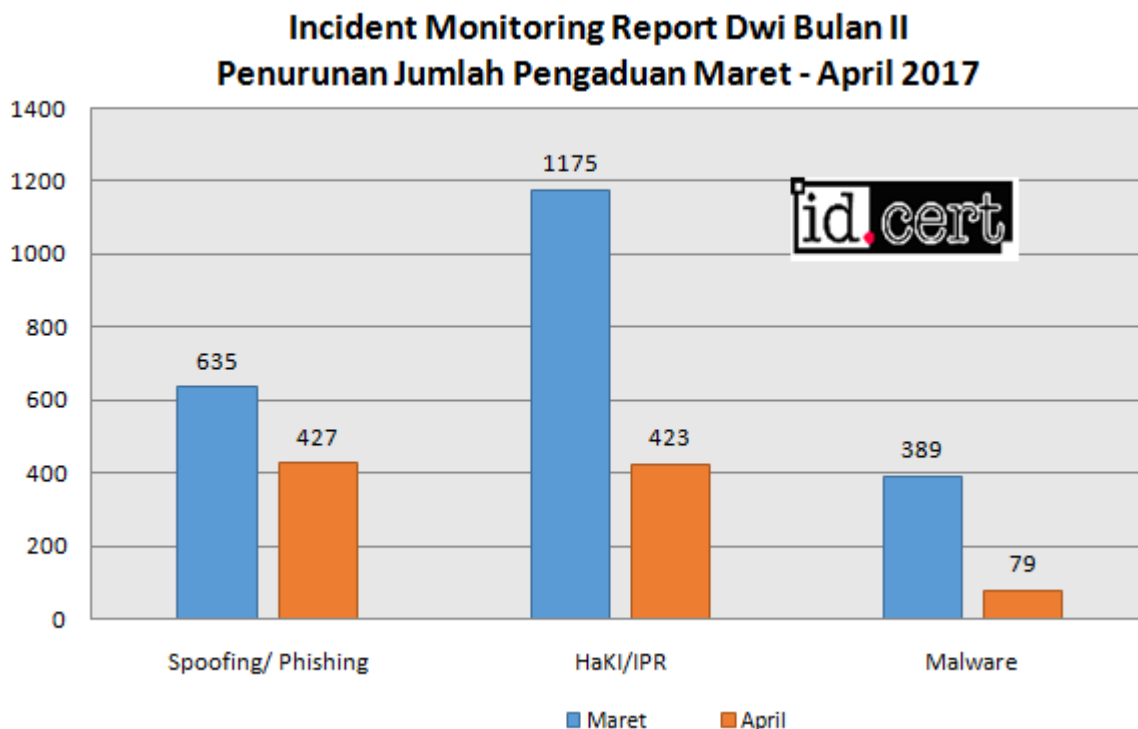
Gambar 4 Peningkatan Jumlah Pengaduan pada bulan Maret – April 2017

3.2 Kelompok Pengaduan yang Mengalami Penurunan

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

1. *Spoofing/phishing* mengalami penurunan jumlah pengaduan dari 635 pada bulan Maret dan turun sebesar 32,76% di bulan April dengan jumlah pengaduan sebanyak 427.
2. Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR) mengalami penurunan jumlah pengaduan dari bulan Maret ke April, dari 1.175 turun ke 423. Persentase penurunannya sebesar 64,00%.
3. *Malware* juga mengalami penurunan jumlah pengaduan yang cukup besar secara persentase di bulan April. Jumlah pengaduan di bulan Maret sebanyak 389 dan di bulan April sebanyak 79. Secara persentase penurunan jumlah pengaduan dari bulan Maret ke April mencapai 79,69%.

Grafik penurunan jumlah pengaduan disajikan pada Gambar 5.



Gambar 5 Penurunan Jumlah Pengaduan pada bulan Maret – April 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 sebagaiantisipasi 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. Kementerian 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