

Incident Monitoring Report - 2016

Laporan Dwi Bulanan II 2016

Bulan Maret dan April 2016



April 2016

Daftar Isi

1. Pendahuluan	3
2. Metoda.....	4
3. Uraian	5
3.1 Kelompok Pengaduan yang Mengalami Peningkatan	8
3.2 Kelompok Pengaduan yang Mengalami Penurunan	8
4. Rangkuman.....	10
4.1 Rekomendasi	10
5. Ucapan Terima Kasih.....	11

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-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 Bulan. Laporan ini sebagai paparan gambaran insiden keamanan (*security incident*) yang terjadi selama dua bulan, Maret dan April 2016.

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 II 2016 ini, Spam menempati jumlah pengaduan terbanyak yaitu mencapai 64,02%, sedangkan Network Incident menempati urutan pengaduan kedua dengan persentase jumlah pengaduan sebesar 14,99%. Dilihat dari sisi jumlah pengaduan, terdapat tiga kelompok besar: Spam 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 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), KEMDIKBUD.

2. Metoda

Penyusunan dokumen Dwi Bulan 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 dalam beberapa kategori sebagai berikut :

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.

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.

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_\(electronic\)](http://en.wikipedia.org/wiki/Spam_(electronic))

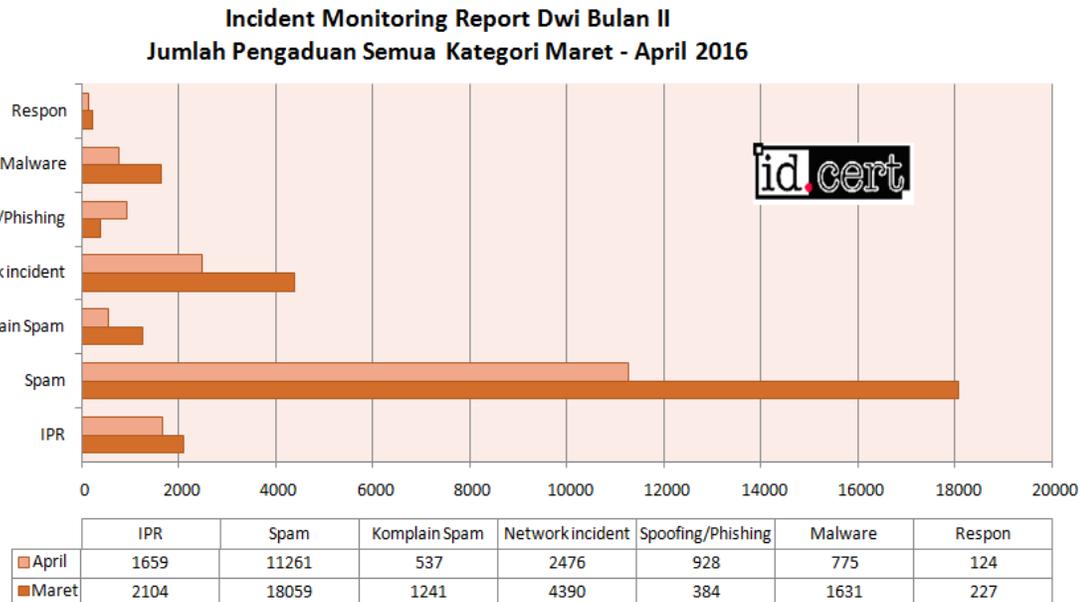
⁵ *Spoofing attack*, http://en.wikipedia.org/wiki/Spoofing_attack

3. Uraian

Email pengaduan yang diterima dikumpulkan berdasarkan kategori pengaduan dan bulan penerimaan laporan, dengan demikian terdapat dua kelompok besar, bulan Maret dan April 2016. 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 II 2016 berdasarkan jumlah pengaduan per bulan ditampilkan pada Gambar 1.



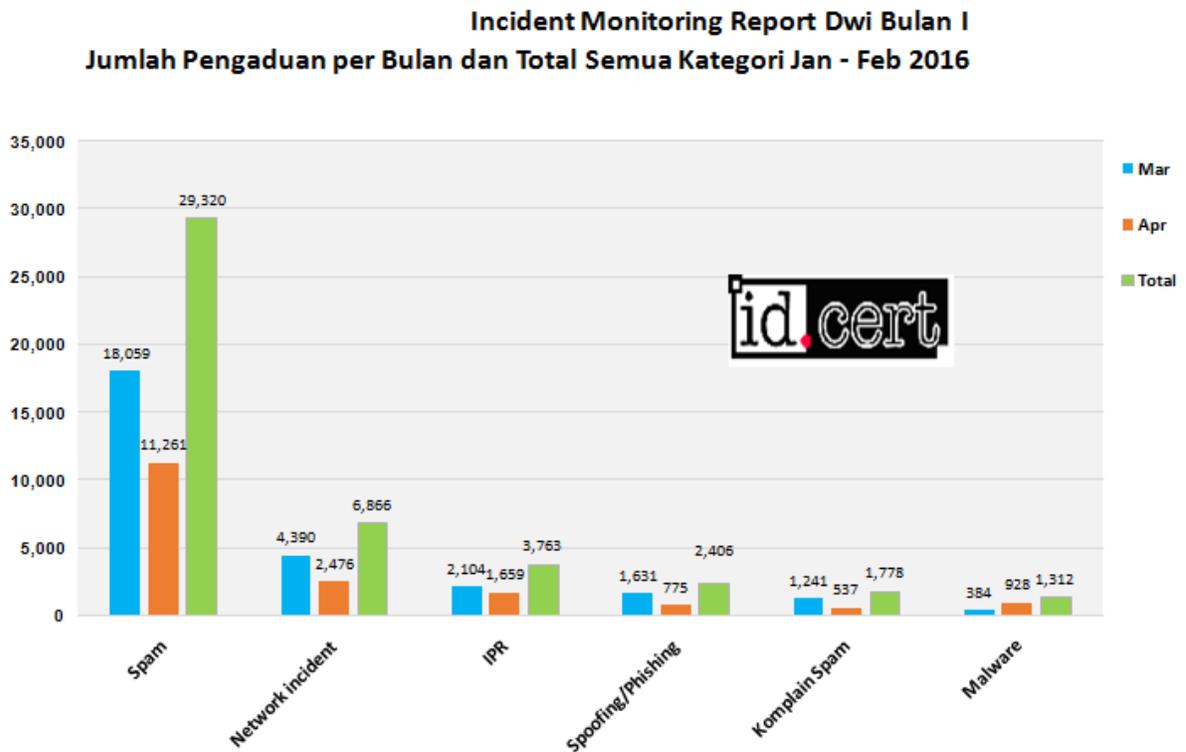
Gambar 1. Jumlah pengaduan semua kategori Maret - April 2016

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 2016

Kategori	Mar	Apr	Total	%
Spam	18,059	11,261	29,320	64.02%
Network incident	4,390	2,476	6,866	14.99%
IPR	2,104	1,659	3,763	8.22%
Spoofing/Phishing	1,631	775	2,406	5.25%
Komplain Spam	1,241	537	1,778	3.88%
Malware	384	928	1,312	2.86%
Respon	227	124	351	0.77%

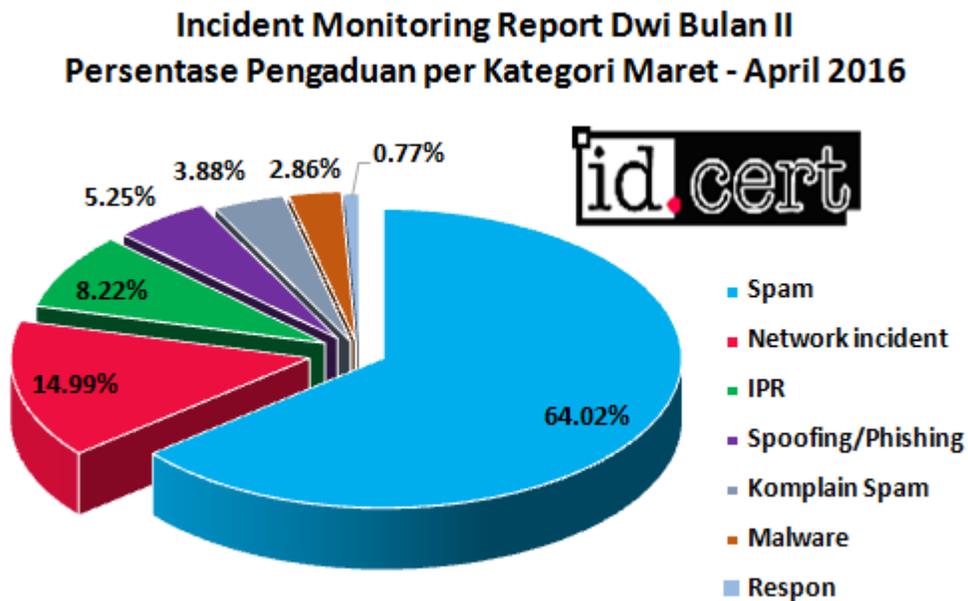
Pada Gambar 2 dapat dilihat perkembangan ataupun penurunan dari jumlah pengaduan antara bulan Maret - April 2016 dan jumlah total dua bulan.



Gambar 2. Jumlah pengaduan per bulan dan total semua kategori Maret - April 2016

Perhitungan perkembangan dilakukan terhadap jumlah pengaduan pada bulan pertama Maret, bulan kedua April dan bernilai negatif jika terjadi penurunan. Tren untuk Dwi Bulan II ini yaitu, masing-masing kategori mengalami penurunan jumlah pengaduan pada bulan April. 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 II 2016

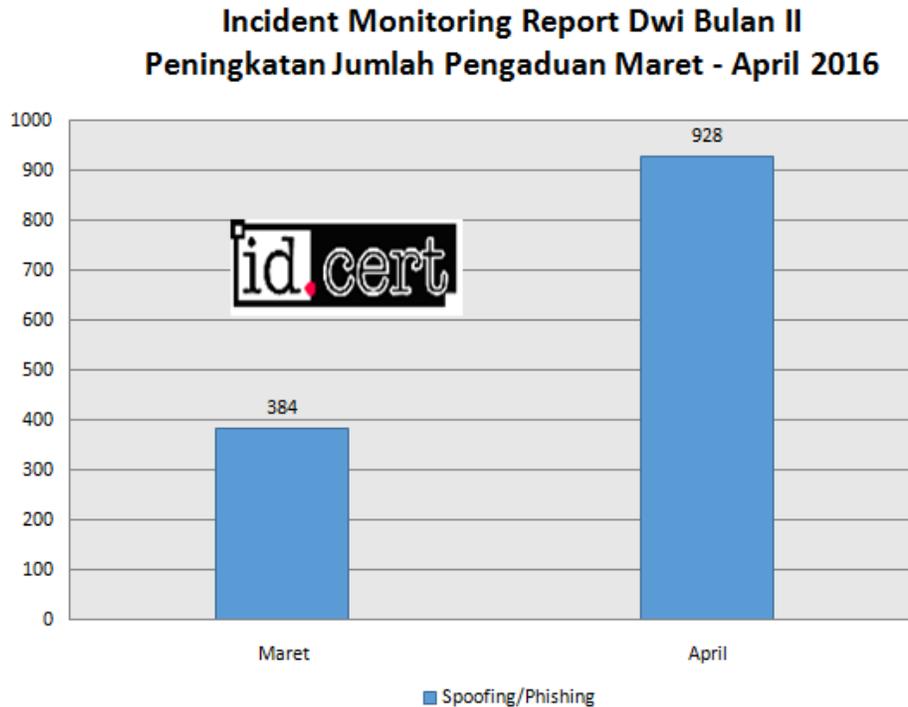
Untuk mengetahui perkembangan naik maupun turun dalam bentuk persentase dapat dilihat pada Tabel 2 berikut.

Tabel 2. Perkembangan jumlah pengaduan dalam persentase

Kategori	Maret	April	%
Spoofing/Phishing	384	928	141.67%
IPR	2104	1659	-21.15%
Spam	18059	11261	-37.64%
Network incident	4390	2476	-43.60%
Respon	227	124	-45.37%
Malware	1631	775	-52.48%
Komplain Spam	1241	537	-56.73%

3.1 Kelompok Pengaduan yang Mengalami Peningkatan

Dari sekian banyak kategori pengaduan, terdapat kategori yang mengalami peningkatan jumlah pengaduan dari yaitu Spoofing/Phishing. Kategori ini meningkat sebesar 141,67% dari bulan Maret ke April dengan jumlah pengaduan bulan Maret sebanyak 384 dan April sebanyak 928 pengaduan. Grafik peningkatan pengaduan tersebut disajikan pada Gambar 4.



Gambar 4 Peningkatan Jumlah Pengaduan pada bulan Maret – April 2016

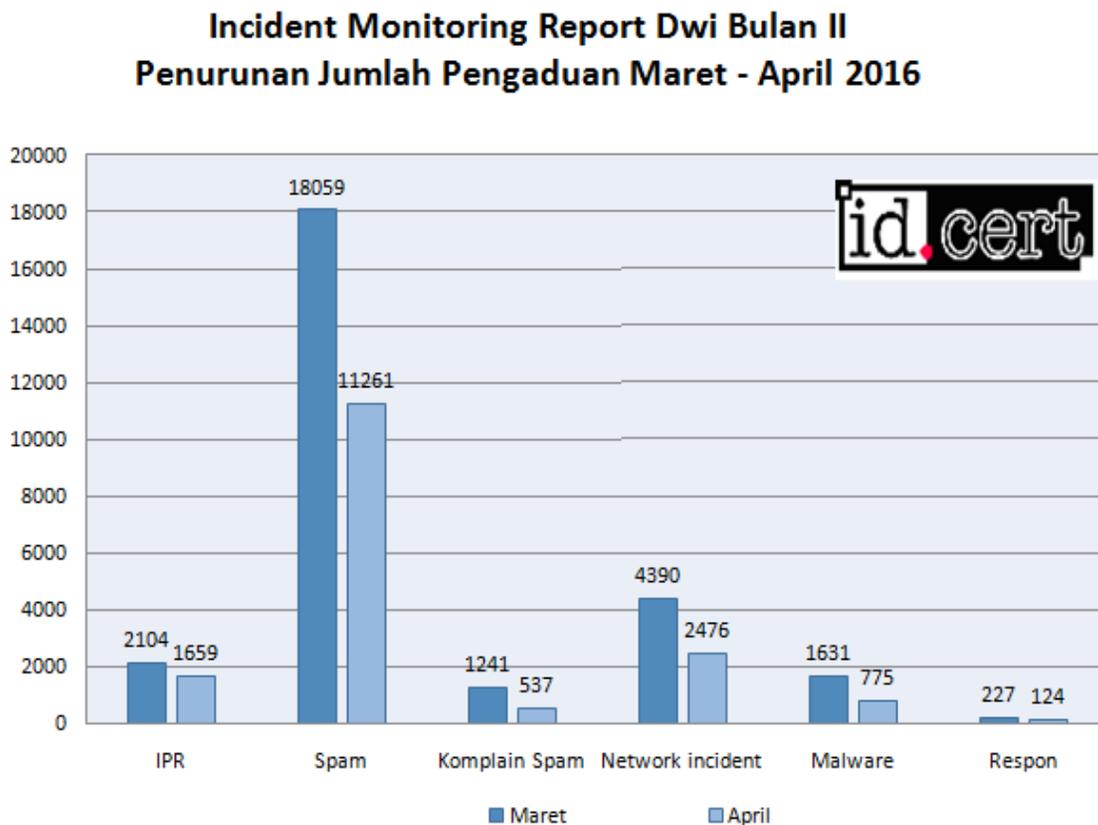
3.2 Kelompok Pengaduan yang Mengalami Penurunan

Pada bulan Maret – April terdapat kategori yang mengalami penurunan jumlah pengaduan di bulan kedua yaitu:

1. IPR mengalami penurunan jumlah pengaduan dari bulan Maret ke April. Persentase penurunannya mencapai 21,15%.
2. Spam memiliki jumlah pengaduan yang sangat tinggi di bulan Maret dan April. Namun di bulan April terjadi penurunan jumlah pengaduan dibandingkan dengan bulan Maret dengan persentase penurunan sebesar 37,64%.
3. Network incident memiliki jumlah pengaduan sebanyak 4.390 pada bulan Maret dan turun sebesar 43,6% di bulan April dengan jumlah pengaduan sebanyak 2.476.

4. Respon pada bulan Maret berjumlah 227 dan menurun sebesar 45,37% di bulan April dengan jumlah Respon sebanyak 124.
5. Malware memiliki jumlah pengaduan sebesar 1.631 pada bulan Maret dan mengalami penurunan sebesar 52,48% di bulan April dengan jumlah pengaduan sebanyak 775.
6. Komplain Spam mengalami penurunan jumlah pengaduan yang tinggi untuk bulan Maret dan April ini. Persentase penurunan jumlah pengaduan dari bulan Maret ke April sebesar 56,73%.

Grafik penurunan jumlah pengaduan disajikan pada Gambar 5.



Gambar 5 Penurunan Jumlah Pengaduan pada bulan Maret – April 2016

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 menjangkau lebih banyak laporan.

4. Rangkuman

Dengan pertimbangan jumlah pengaduan spam masih 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.

Dua bulan pertama ini Maret dan April, jumlah pengaduan spam masih dominan dibanding kategori lainnya namun 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 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/Postfix⁶ 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. 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