

Incident Monitoring Report - 2015

Laporan Dwi Bulanan IV 2015

Bulan Juli dan Agustus 2015



Agustus 2015

Daftar Isi

1. Pendahuluan	3
2. Metoda.....	4
3. Uraian	5
3.1 Pengaduan yang Mengalami Peningkatan.....	8
3.2 Pengaduan yang Mengalami Penurunan.....	9
4. Rangkuman.....	10
5.1. 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, Juli dan Agustus 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 Bulan IV 2015 ini, IPR menempati jumlah pengaduan terbanyak yaitu mencapai 38,35%, sedangkan Spam menempati urutan pengaduan kedua dengan selisih sekitar 14,68% dari Network Incident yaitu sebesar 29,03%. Dilihat dari sisi jumlah pengaduan, terdapat dua kelompok besar: IPR, Spam, Network Incident, Spoofing/Phishing, dan Malware pada kelompok pertama yang memiliki jumlah pelaporan sedang yaitu di bawah 10.000 di atas 1.000 laporan, dan kelompok kedua yang memiliki jumlah 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 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))

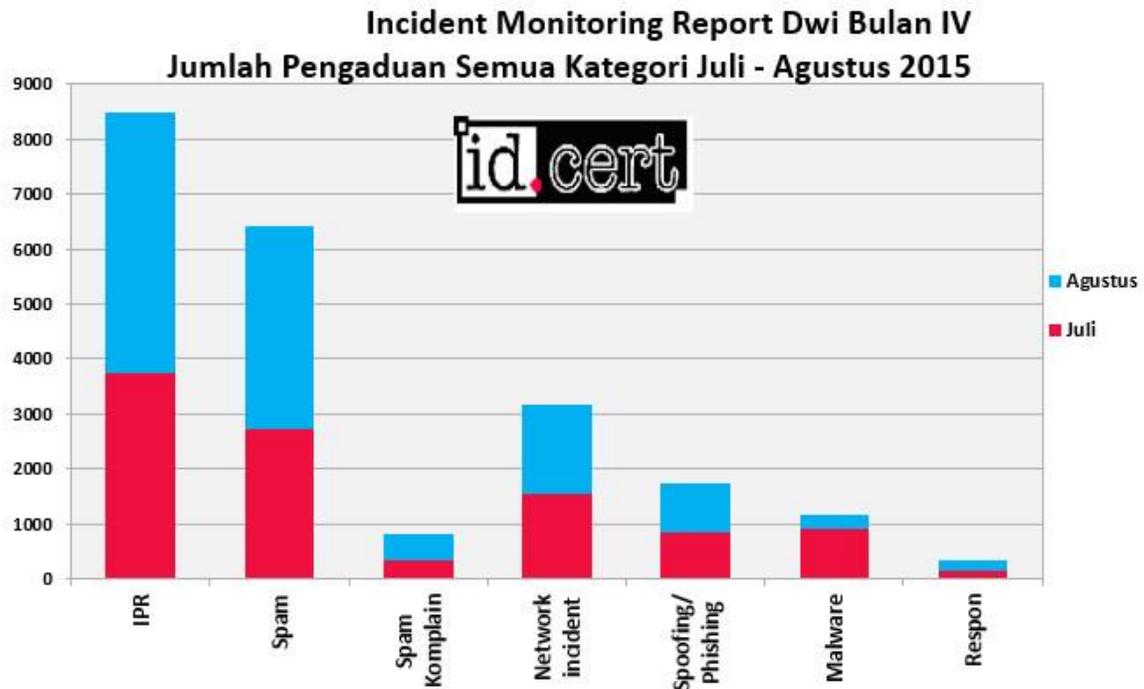
⁵ *Spoofing attack*, http://en.wikipedia.org/wiki/Spoofing_attack

3. Uraian

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



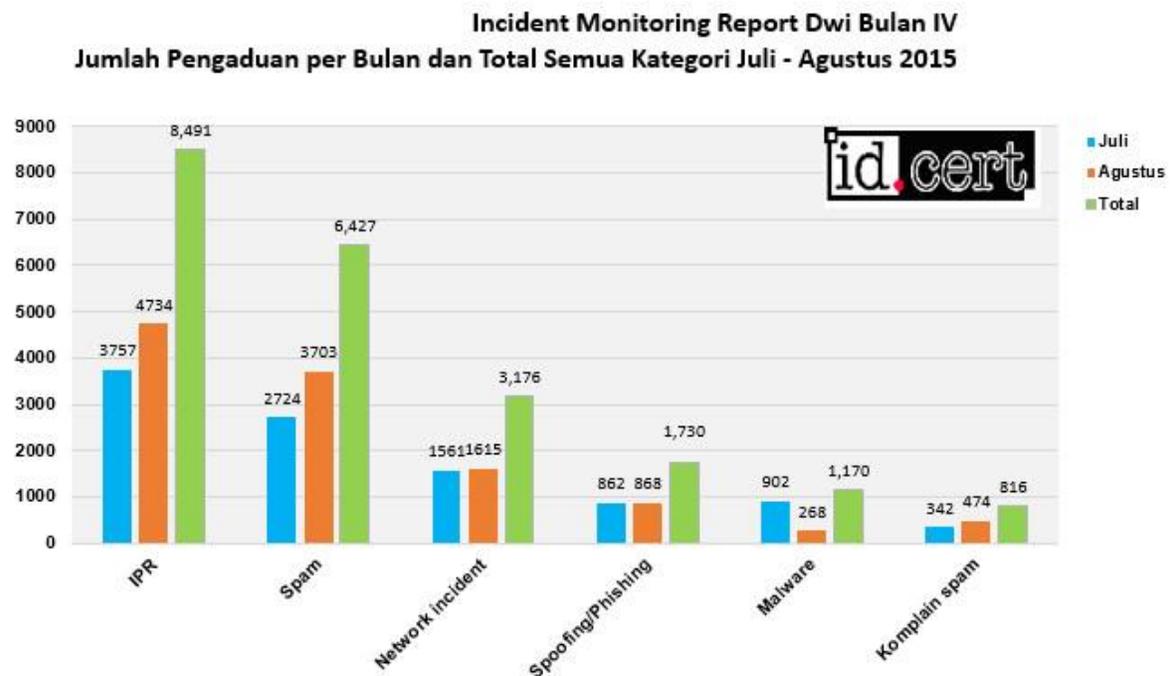
Gambar 1. Jumlah pengaduan semua kategori Juli - Agustus 2015

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 Juli - Agustus 2015

Kategori	Juli	Agustus	Total	%
IPR	3757	4734	8,491	38.35%
Spam	2724	3703	6,427	29.03%
Network incident	1561	1615	3,176	14.34%
Spoofing/Phishing	862	868	1,730	7.81%
Malware	902	268	1,170	5.28%
Komplain spam	342	474	816	3.69%
Respon	134	198	332	1.50%

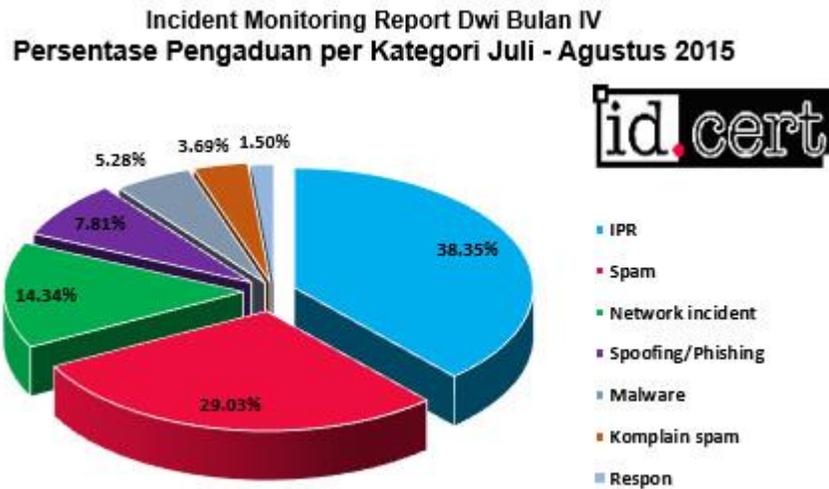
Pada Gambar 2 dapat dilihat perkembangan ataupun penurunan dari jumlah pengaduan antara bulan Juli - Agustus 2015 dan jumlah total dua bulan.



Gambar 2. Jumlah pengaduan per bulan dan total semua kategori Juli - Agustus 2015

Perhitungan perkembangan dilakukan terhadap jumlah pengaduan pada bulan pertama Juli, bulan kedua Agustus dan bernilai negatif jika terjadi penurunan. Tren untuk dwi bulan ini yaitu, masing-masing kategori mengalami peningkatan jumlah pengaduan pada bulan Agustus. 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.

Tabel 2. Perkembangan jumlah pengaduan dalam persentase

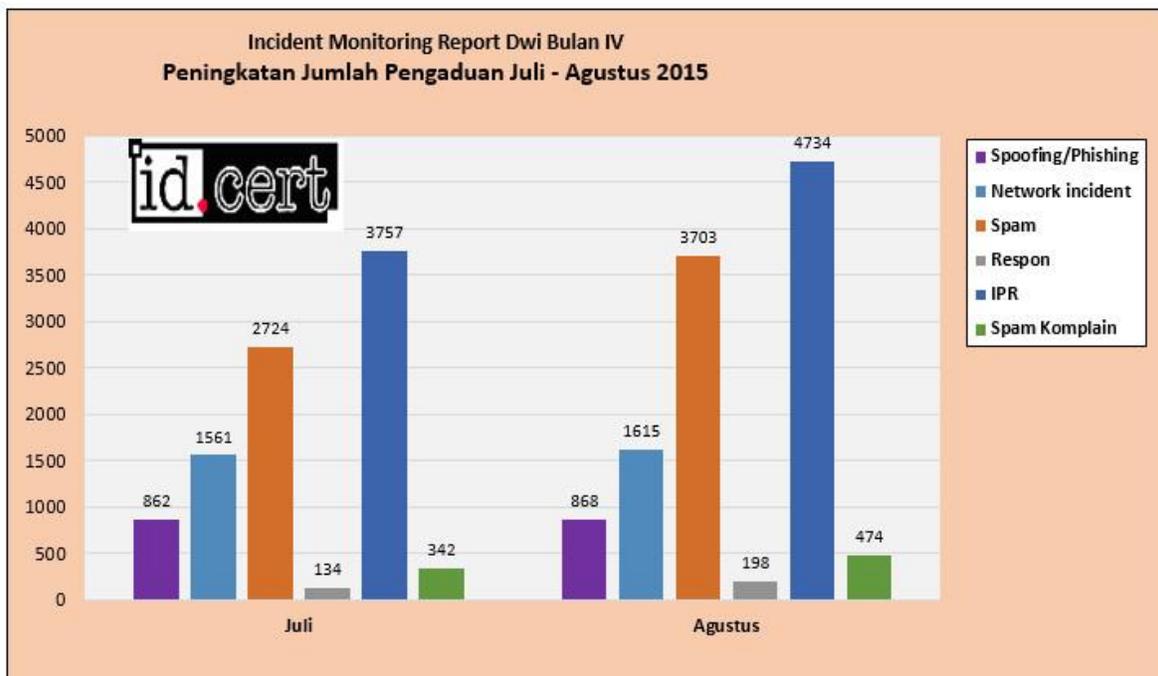
Kategori	Juli	Agustus	%
Respon	134	198	47.76%
Spam Komplain	342	474	38.60%
Spam	2724	3703	35.94%
IPR	3757	4734	26.00%
Network incident	1561	1615	3.46%
Spoofing/ Phishing	862	868	0.70%
Malware	902	268	-70.29%

3.1 Pengaduan yang Mengalami Peningkatan

Dari sekian banyak kategori pengaduan, terdapat kategori yang mengalami peningkatan jumlah pengaduan yaitu:

1. Spoofing/Phishing mempunyai jumlah pengaduan sebesar 862 di bulan Juli, naik menjadi 1.246 pada bulan Agustus dengan persentase peningkatan sebesar 0,7%.
2. Network Incident mempunyai jumlah pengaduan sebesar 1.561 di bulan Juli, naik menjadi 1.625 pada bulan Agustus dengan persentase peningkatan sebesar 3,46%.
3. Spam mempunyai jumlah pengaduan sebesar 2.724 di bulan Juli, naik menjadi 3.703 pada bulan Agustus dengan persentase peningkatan sebesar 35,94%.
4. Respon mempunyai jumlah pengaduan sebesar 134 di bulan Juli, naik menjadi 198 pada bulan Agustus dengan persentase peningkatan sebesar 47,76%.
5. IPR mempunyai jumlah pengaduan sebesar 3.757 di bulan Juli, naik menjadi 4.734 pada bulan Agustus dengan persentase peningkatan sebesar 26%.
6. Spam Komplain mempunyai jumlah pengaduan sebesar 342 di bulan Juli, naik menjadi 474 pada bulan Agustus dengan persentase peningkatan sebesar 38,6%.

Grafik peningkatan pengaduan tersebut disajikan pada Gambar 4.

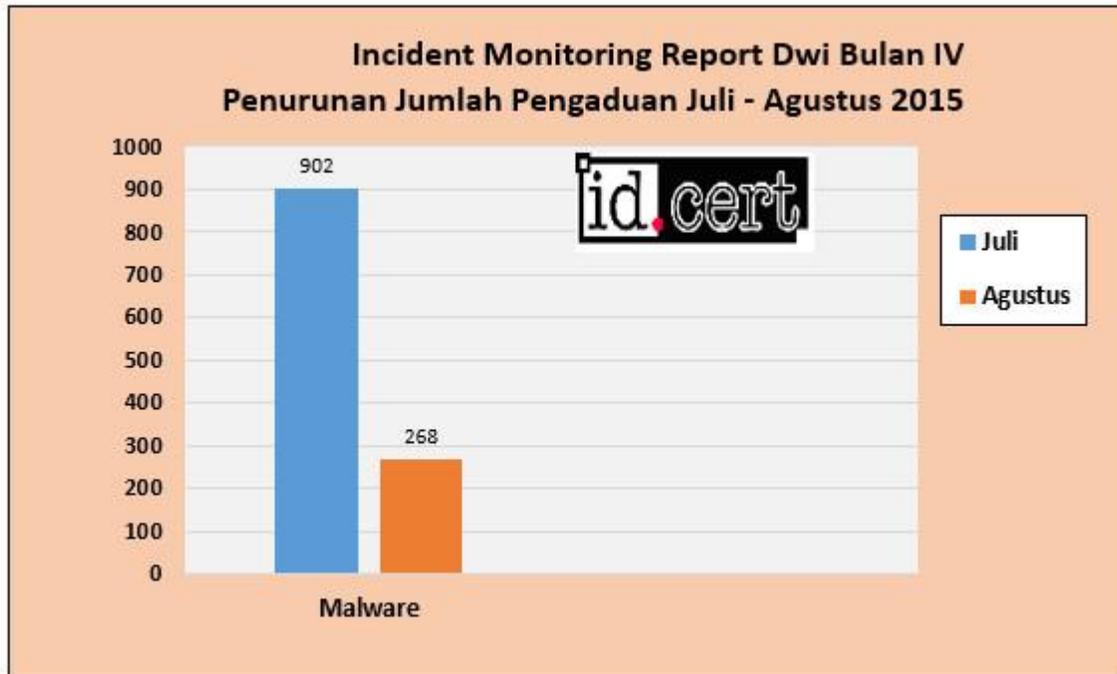


Gambar 4 Peningkatan Jumlah Pengaduan pada bulan Juli – Agustus 2015

3.2 Pengaduan yang Mengalami Penurunan.

Pada bulan Juli – Agustus terdapat kategori yang mengalami penurunan jumlah pengaduan, yaitu Malware. Jumlah pengaduan Malware pada bulan Juli sebesar 902, mengalami penurunan pada bulan Agustus menjadi 268. Persentase penurunan jumlah pengaduan Malware yaitu 70,29%.

Grafik penurunan jumlah pengaduan disajikan pada Gambar 5.



Gambar 5 Penurunan Jumlah Pengaduan pada bulan Juli – Agustus 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 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 keempat ini, Juli dan Agustus, jumlah pengaduan IPR masih 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.

5.1. 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. KEMENDIKBUD