Incident Monitoring Report - 2017

Laporan Dwi Bulan V 2017

Bulan September dan Oktober 2017

November 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 Bulan. Laporan ini sebagai paparan gambaran insiden keamanan (*security incident*) yang terjadi selama dua bulan, September dan Oktober 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 Bulan V 2017 ini, *Spam* menempati jumlah pengaduan terbanyak yaitu mencapai 41,13% atau berjumlah total 17.464 aduan. Dilihat dari sisi jumlah pengaduan, terdapat dua kelompok: *Spam* dan HaKI/IPR (Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR)) pada kelompok pertama yang memiliki jumlah pelaporan di atas 10.000 laporan, dan Komplain *Spam, Network Incident*, *Malware*, *Spoofing/Phishing*, dan Respon pada kelompok kedua yang berjumlah pengaduan rendah yaitu di bawah 10.000 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 Bulan V 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`

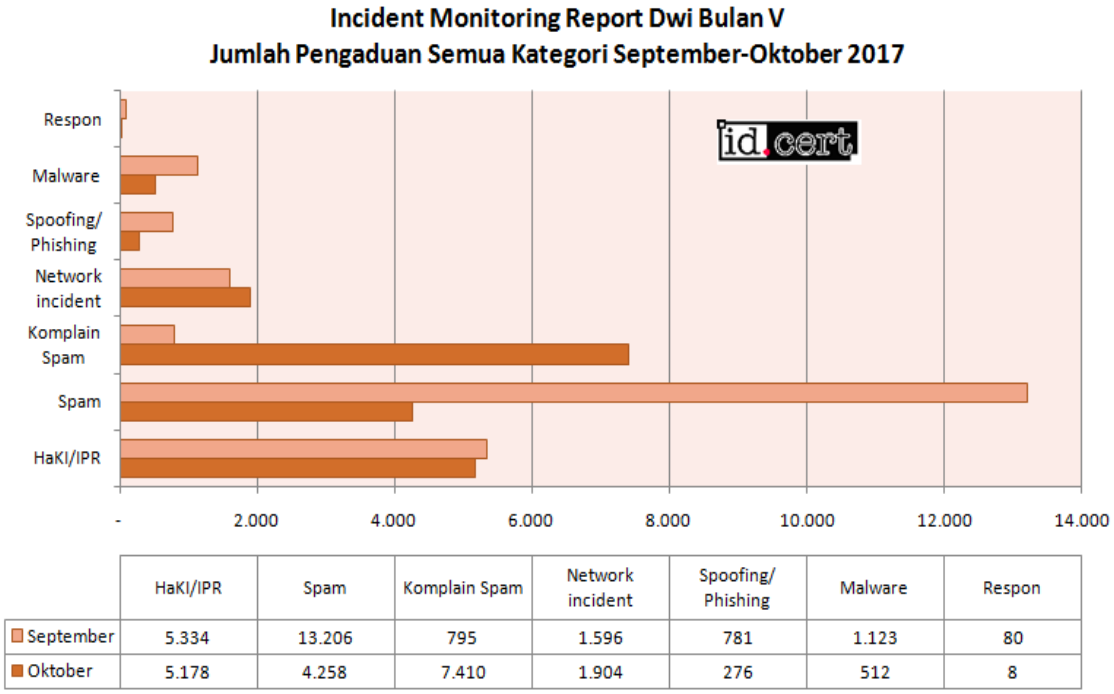
3. Uraian

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



	HaKI/IPR	Spam	Komplain Spam	Network incident	Spoofing/ Phishing	Malware	Respon
September	5.334	13.206	795	1.596	781	1.123	80
Oktober	5.178	4.258	7.410	1.904	276	512	8

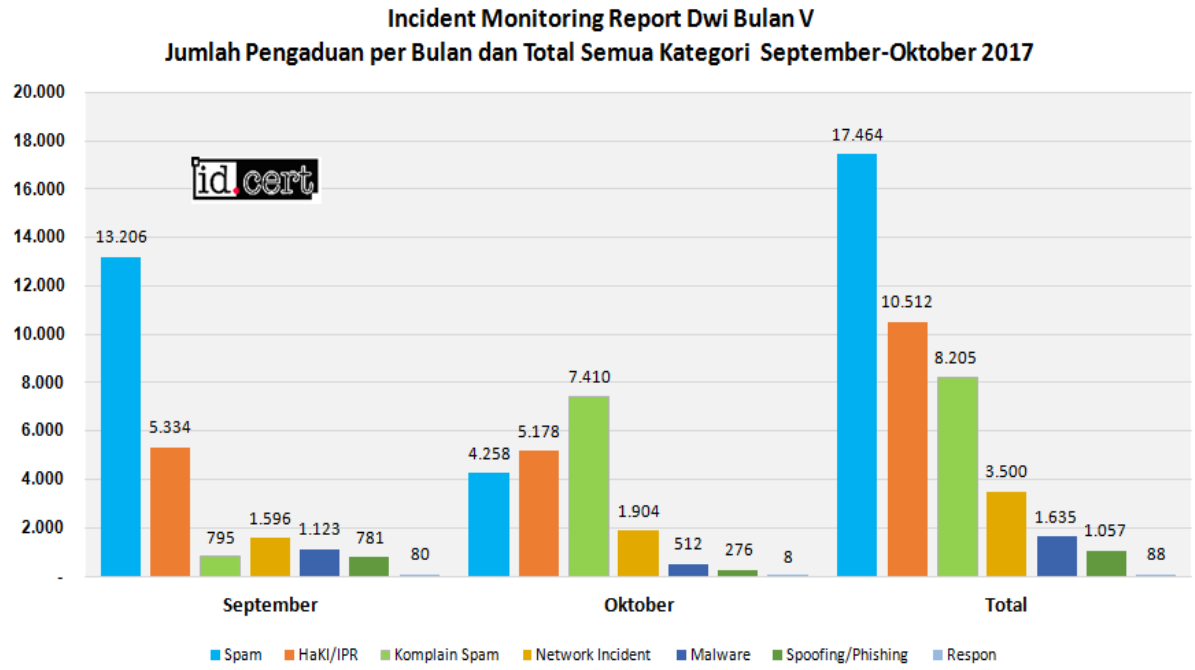
Gambar 1 Jumlah pengaduan semua kategori September-Oktober 2017

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 September-Oktober 2017

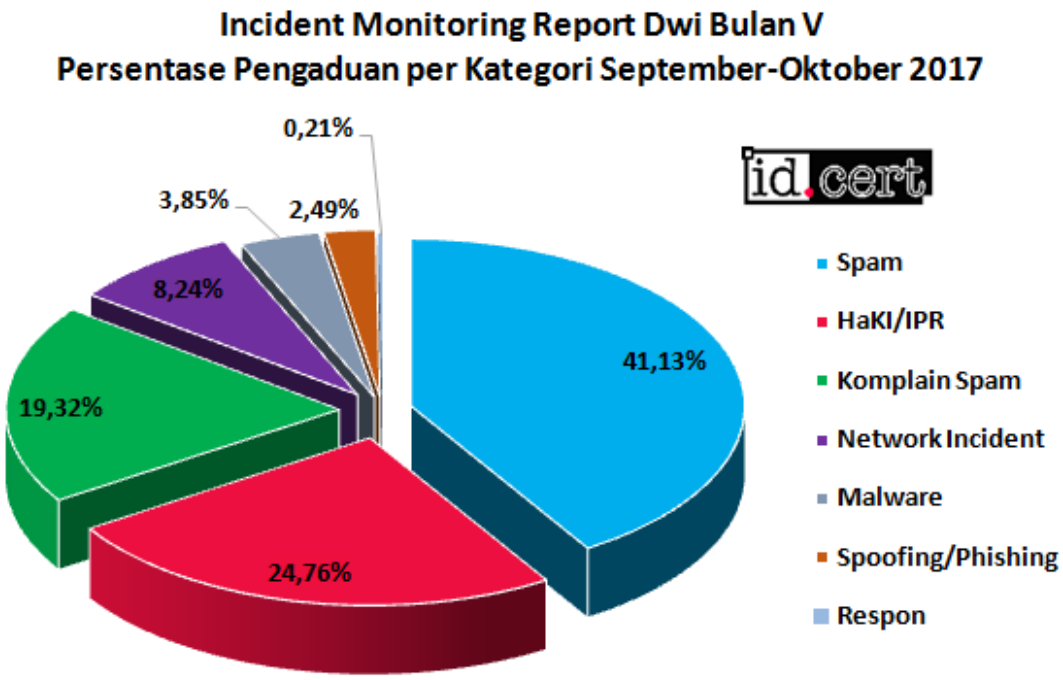
Kategori	September	Oktober	Total	%
Spam	13.206	4.258	17.464	41,13%
HaKI/IPR	5.334	5.178	10.512	24,76%
Komplain Spam	795	7.410	8.205	19,32%
Network Incident	1.596	1.904	3.500	8,24%
Malware	1.123	512	1.635	3,85%
Spoofing/Phishing	781	276	1.057	2,49%
Respon	80	8	88	0,21%

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



Gambar 2 Jumlah pengaduan per bulan dan total semua kategori September-Oktober 2017

Perhitungan perkembangan dilakukan terhadap jumlah pengaduan pada bulan pertama September, bulan kedua Oktober dan bernilai negatif jika terjadi penurunan. Tren untuk Dwi Bulan V ini yaitu sebagian kategori mengalami peningkatan dan sebagian kategori lain mengalami penurunan jumlah pengaduan pada bulan Oktober. 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 Bulan V 2017

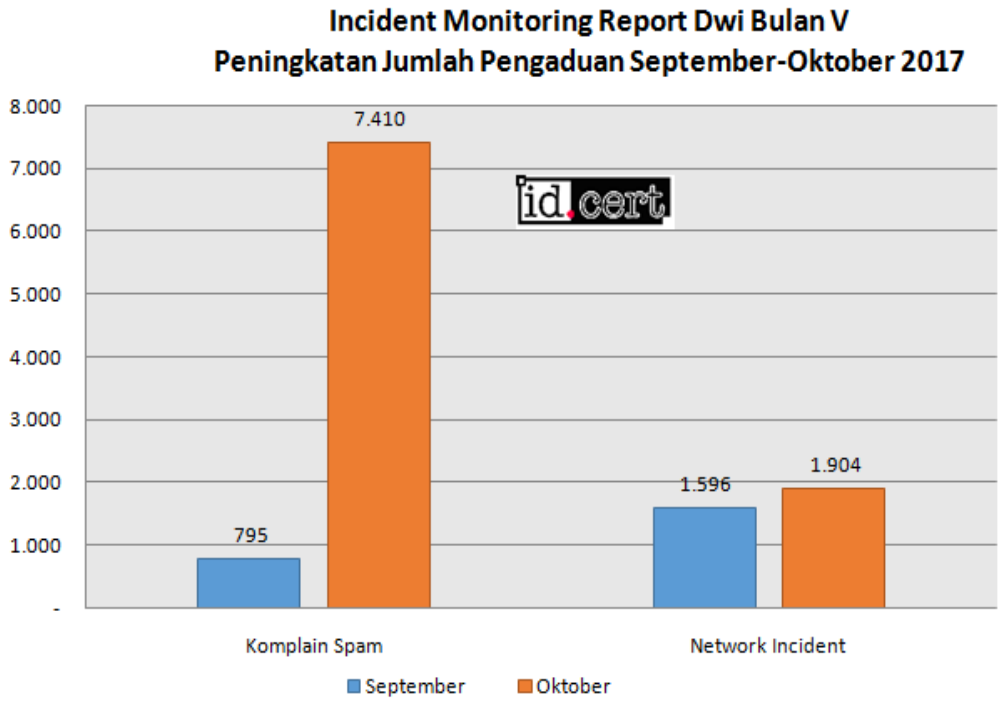
Untuk mengetahui perkembangan naik maupun turun dalam bentuk persentase dapat dilihat pada Tabel 2 berikut.

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

Kategori	September	Oktober	%
Komplain Spam	795	7.410	832,08%
Network Incident	1.596	1.904	19,30%
HaKI/IPR	5.334	5.178	-2,92%
Malware	1.123	512	-54,41%
Spoofing/Phishing	781	276	-64,66%
Spam	13.206	4.258	-67,76%
Respon	80	8	-90,00%

3.1 Kelompok Pengaduan yang Mengalami Peningkatan

Grafik peningkatan jumlah pengaduan selama bulan September dan Oktober disajikan pada Gambar 4.



Gambar 4 Peningkatan Jumlah Pengaduan pada bulan September-Oktober 2017

Dari sekian banyak kategori pengaduan, terdapat 2 (dua) kategori yang mengalami peningkatan jumlah pengaduan, yaitu:

1. Komplain *Spam*

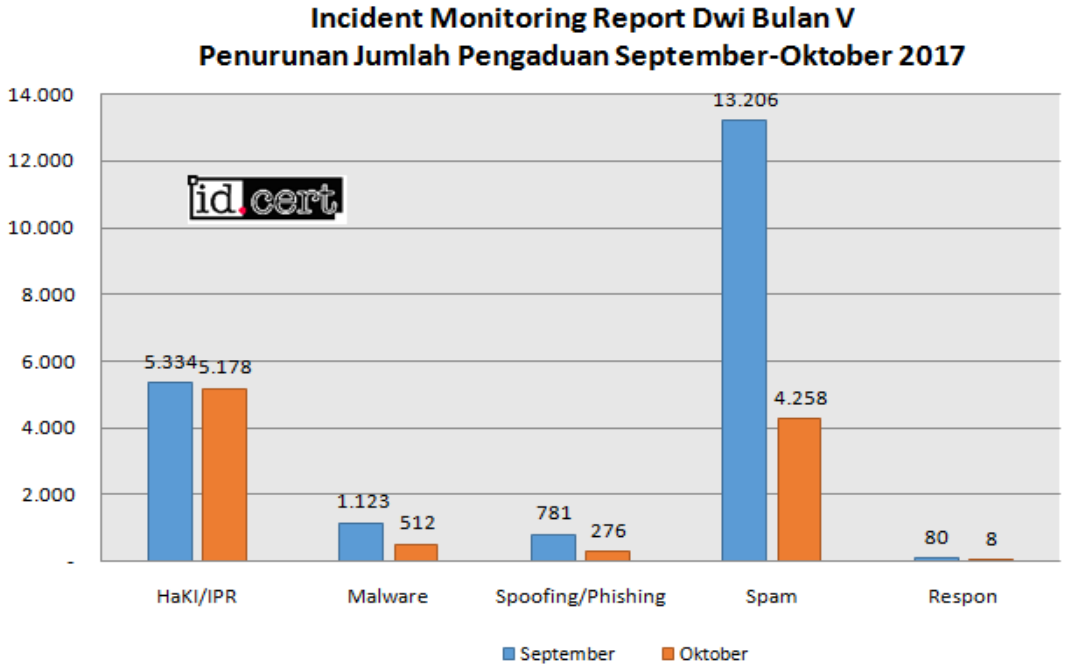
Komplain *Spam* mengalami lonjakan peningkatan jumlah yang sangat tinggi dari bulan September ke Oktober ini, yaitu 6.615 pengaduan. Komplain *Spam* memiliki jumlah sebanyak 795 pada bulan September dan naik dengan persentase sebesar 832,08% di bulan Oktober dengan jumlah sebanyak 7.410. Komplain *Spam* adalah aduan *spam* yang diterima oleh user di Indonesia.

2. *Network Incident*

Network Incident jumlah pengaduannya meningkat 19,30% di bulan kedua. Di bulan pertama September jumlahnya sebesar 1.596 meningkat sebanyak 308 menjadi 1.904 pengaduan di bulan kedua Oktober.

3.2 Kelompok Pengaduan yang Mengalami Penurunan

Grafik penurunan jumlah pengaduan selama bulan September dan Oktober disajikan pada Gambar 5.



Gambar 5 Penurunan Jumlah Pengaduan pada bulan September-Oktober 2017

Bulan September – Oktober 2017 terdapat 5 (lima) kategori yang mengalami penurunan jumlah pengaduan di bulan kedua, yaitu:

1. HaKI/IPR

Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR) mengalami penurunan jumlah pengaduan dari bulan September ke Oktober, dari 5.334 turun menjadi

5.178. Persentase penurunannya sebesar 2,92% atau 156 jumlah pengaduan. Aduan HaKI/IPR sebagian besar adalah pengunduhan film secara ilegal di IP Address Indonesia.

2. *Malware*

Malware mengalami penurunan jumlah pengaduan sebesar 54,41%, yaitu 611 pengaduan. Penurunan jumlah sebesar 611 pengaduan tersebut ketika pada bulan September berjumlah 1.123 pengaduan dan pada bulan Oktober menurun menjadi 512 pengaduan.

3. *Spoofing/Phishing*

   Spoofing/Phishing juga mengalami penurunan jumlah pengaduan dari 781 pada bulan September dan turun sebesar 64,66%, yaitu 505, di bulan Oktober dengan jumlah pengaduan sebanyak 276.

4. *Spam*

   Meskipun *Spam* memiliki jumlah pengaduan total terbanyak selama bulan September dan Oktober, tetapi mengalami penurunan jumlah pengaduan di bulan kedua, yaitu bulan Oktober. Jumlah pengaduan *Spam* sebesar 13.206 di bulan September mengalami penurunan sebesar 8.948 menjadi 4.258 di bulan Oktober. Persentase penurunannya mencapai sebesar 67,76%.

5. Respon

   Respon memiliki jumlah pengaduan sejumlah 80 di bulan September. Pada bulan Oktober menurun jumlah pengaduan dibandingkan dengan bulan September menjadi 8 dengan persentase penurunan sebesar 90,00%.

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