Incident Monitoring Report - 2015

Laporan Dwi Bulanan V 2015

Bulan September dan Oktober 2015

Oktober 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 11
5. Ucapan Terima Kasih 12

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-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 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 V 2015 ini, IPR menempati jumlah pengaduan terbanyak yaitu mencapai 57,84%, sedangkan Spam menempati urutan pengaduan terbanyak kedua dengan jumlah 31,04%. Dilihat dari sisi jumlah pengaduan, terdapat tiga kelompok besar: IPR dan 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), 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 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.

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.

---

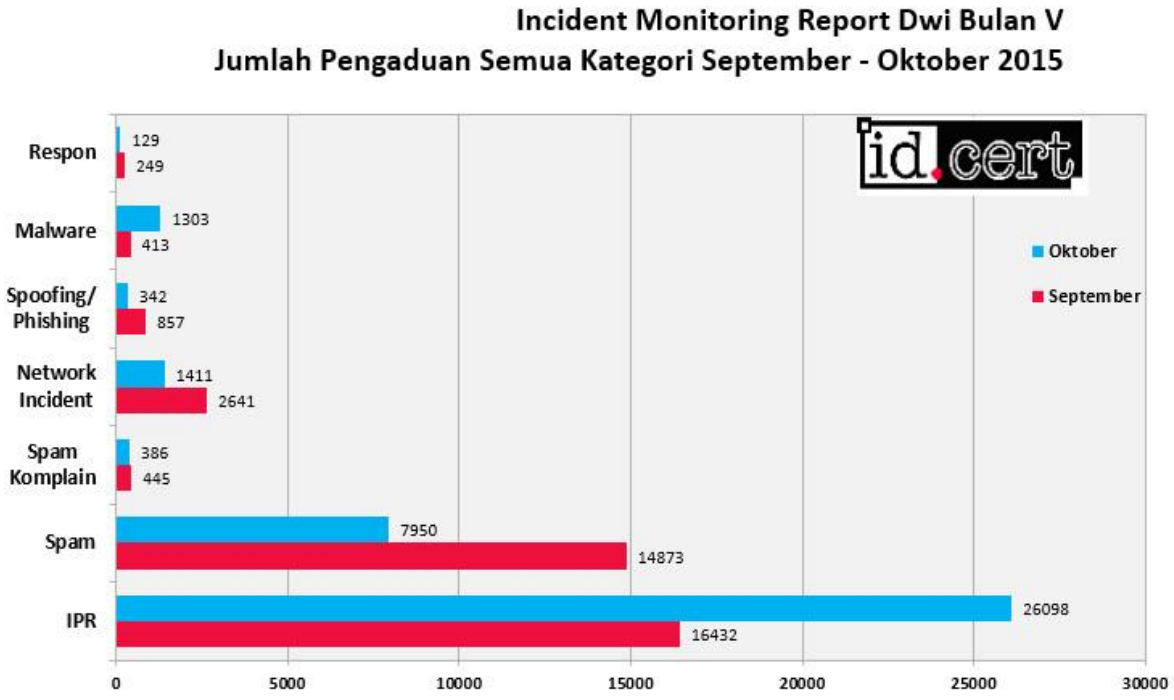
[2] *Fraud*, `http://en.wikipedia.org/wiki/Fraud`
[3] *Malware*, `http://en.wikipedia.org/wiki/Malware`
[4] *Spam (electronic)*, `http://en.wikipedia.org/wiki/Spam_(electronic)`
[5] *Spoofing attack*, `http://en.wikipedia.org/wiki/Spoofing_attack`

3. Uraian

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



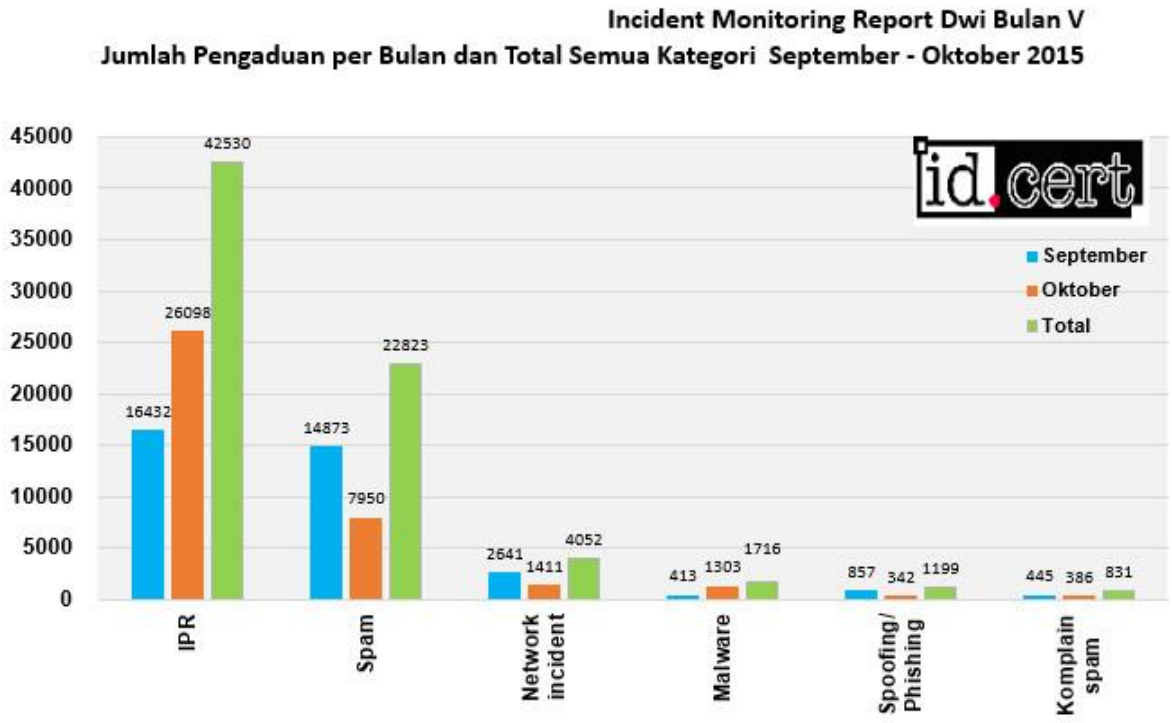
Gambar 1. Jumlah pengaduan semua kategori September - Oktober 2015

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 September - Oktober 2015

Kategori	September	Oktober	Total	%
IPR	16432	26098	42530	57.84%
Spam	14873	7950	22823	31.04%
Network incident	2641	1411	4052	5.51%
Malware	413	1303	1716	2.33%
Spoofing/ Phishing	857	342	1199	1.63%
Komplain spam	445	386	831	1.13%
Respon	249	129	378	0.51%

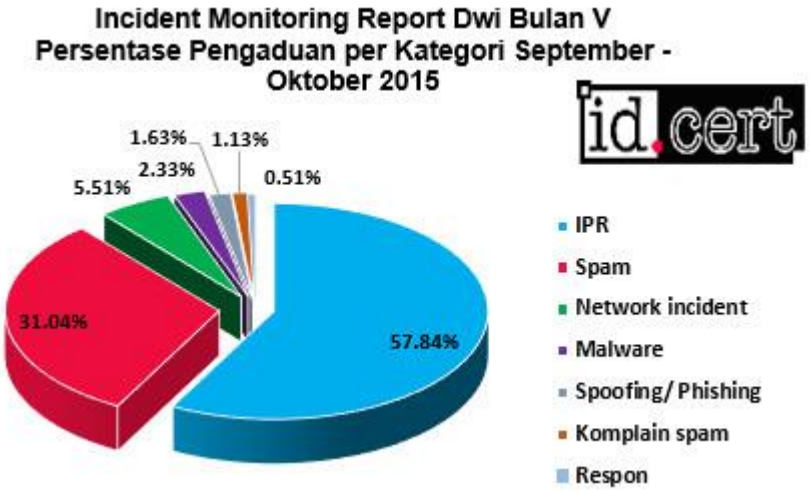
Pada Gambar 2 dapat dilihat perkembangan ataupun penurunan dari jumlah pengaduan antara bulan September - Oktober 2015 dan jumlah total dua bulan.



Gambar 2. Jumlah pengaduan per bulan dan total semua kategori September - Oktober 2015

Perhitungan perkembangan dilakukan terhadap jumlah pengaduan pada bulan pertama September, bulan kedua Oktober dan bernilai negatif jika terjadi penurunan. Tren untuk dwi bulan ini yaitu, masing-masing kategori mengalami penurunan jumlah pengaduan pada bulan Oktober. 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	September	Oktober	%
Malware	413	1303	215.50%
IPR	16432	26098	58.82%
Spam Komplain	445	386	-13.26%
Spam	14873	7950	-46.55%
Network incident	2641	1411	-46.57%
Respon	249	129	-48.19%
Spoofing/ Phishing	857	342	-60.09%

3.1 Pengaduan yang mengalami peningkatan

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

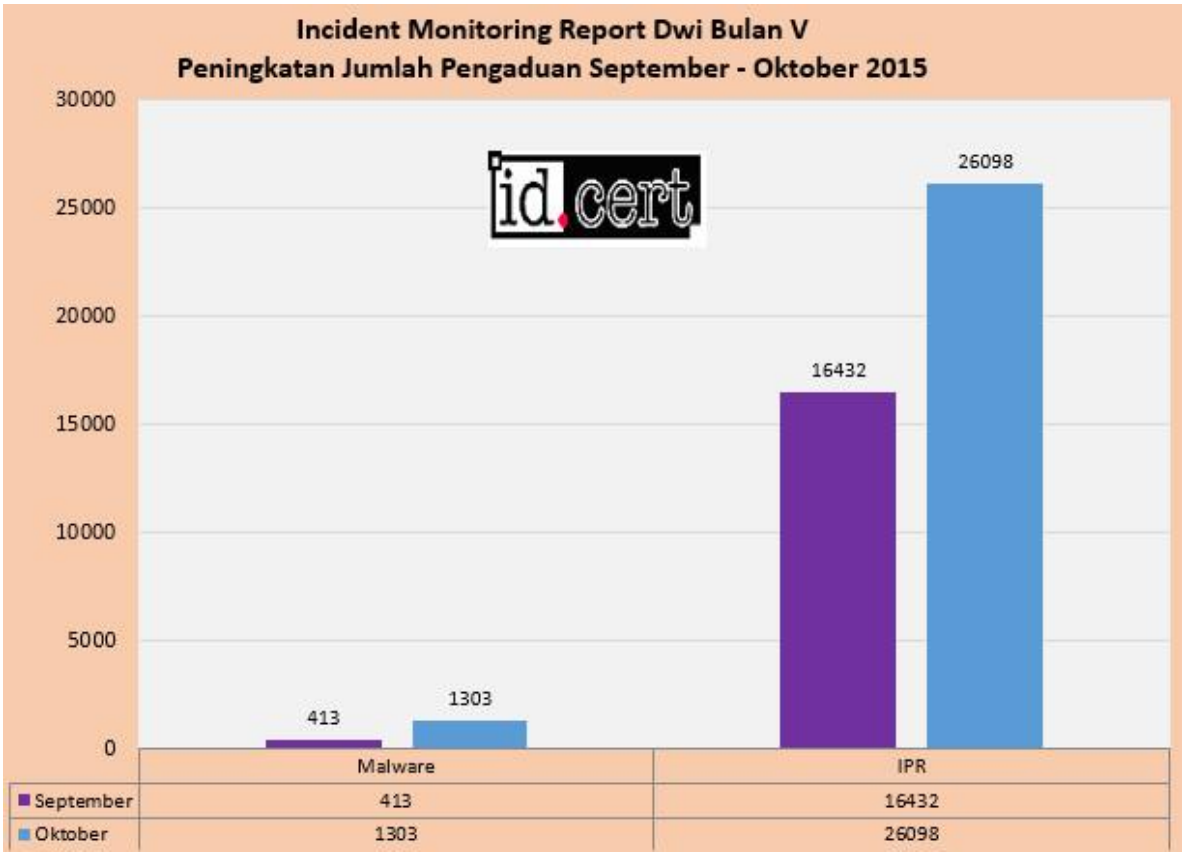
1. Malware

   Pada bulan Oktober, jumlah pengaduan malware meningkat hingga 215,5% dibanding bulan sebelumnya. Jumlah pengaduan malware pada bulan September sebesar 413 dan meningkat drastis dengan jumlah pengaduan bulan Oktober sebesar 1303.

2. IPR

   Persentase peningkatan jumlah pengaduan IPR dari bulan September hingga Oktober yaitu sebesar 58,82%. Pada bulan September, IPR memiliki jumlah pengaduan sebesar 16432 dan meningkat pada bulan Oktober dengan jumlah pengaduan sebesar 26098.

Grafik peningkatan pengaduan tersebut disajikan pada Gambar 4.



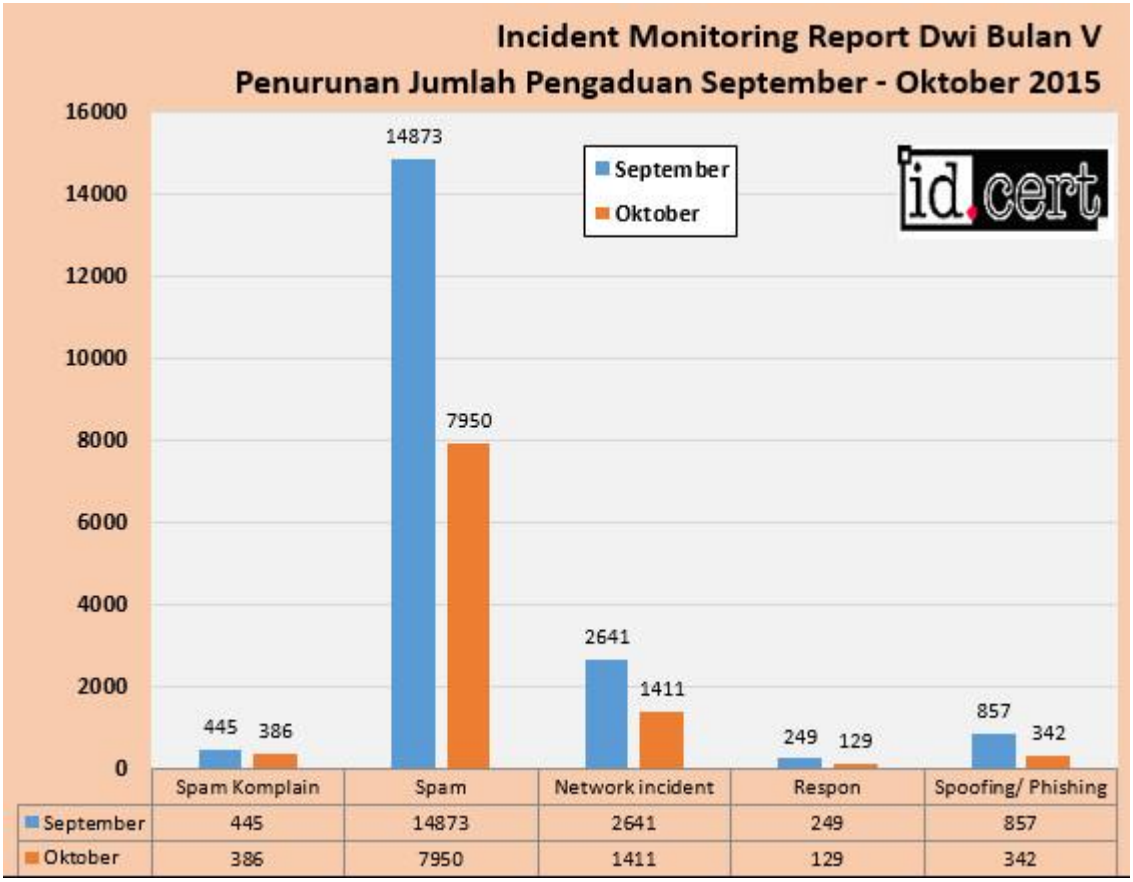
Gambar 4 Peningkatan Jumlah Pengaduan pada bulan September – Oktober 2015

3.2 Pengaduan yang mengalami penurunan

Pada bulan September – Oktober terdapat kategori yang mengalami penurunan jumlah pengaduan, yaitu Spam Komplain, Spam, Network Incident, Respon, dan Spoofing/Phishing. Berikut uraian masing-masing kategori yang mengalami penurunan.

1. Spam. Pada bulan September, jumlah pengaduan spam sangat tinggi sebesar 14873 pengaduan. Namun mengalami penurunan jumlah pengaduan sebesar 46,55% pada bulan Oktober.
2. Network Incident. Persentase penurunan jumlah pengaduan network incident pada dwi bulan V ini sebesar 46,57%. Jumlah pengaduan kategori ini di bulan September sebesar 2641 dan turun menjadi 1411 di bulan Oktober.
3. Spoofing/Phishing. Pada bulan September, spoofing/phishing memiliki jumlah pengaduan sebanyak 857. Kategori ini mengalami penurunan jumlah pengaduan yang cukup tinggi dengan persentase penurunan jumlah sebesar 60,09% di bulan Oktober.
4. Spam Komplain. Pada bulan September, jumlah pengaduan komplain spam sebesar 445 pengaduan. Namun mengalami penurunan jumlah pengaduan sebesar 13,26% pada bulan Oktober.
5. Respon. Persentase penurunan jumlah respon pada dwi bulan V ini sebesar 48,19%. Jumlah pengaduan kategori ini di bulan September sebesar 249 dan turun menjadi 149 di bulan Oktober.

Grafik penurunan jumlah pengaduan disajikan pada Gambar 5.



Gambar 5 Penurunan Jumlah Pengaduan pada bulan September – Oktober 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, September dan Oktober, 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/Postfix[6] 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. 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. KEMENDIKBUD