Incident Monitoring Report - 2017

Laporan Dwi Bulanan I 2017

Bulan Januari dan Februari 2017

Maret 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 Bulanan. Laporan ini sebagai paparan gambaran insiden keamanan (*security incident*) yang terjadi selama dua bulan, Januari dan Februari 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

[1] Indonesia Computer Emergency Response Team

diterima memberi gambaran bagian-bagian yang perlu dibenahi, keterkaitan antar lembaga, dan untuk membantu penyusunan rencana ke depan.

Pada laporan Dwi Bulanan I 2017 ini, *Spam* menempati jumlah pengaduan terbanyak yaitu mencapai 37,05% atau berjumlah total 6.176 aduan. Dilihat dari sisi jumlah pengaduan, terdapat dua kelompok: *Spam*, Komplain Spam, HaKI/IPR, dan *Network Incident*, pada kelompok pertama yang memiliki jumlah pelaporan di atas 1.000 laporan, dan *Spoofing/Phishing*, *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 40 (empat puluh) responden yang terdiri dari: Kominfo, ID-CERT, PANDI, APJII, Detik.net, Zone-h dan Anti Fraud Command Center (AFCC), 3 (tiga) operator telekomunikasi, 7 (tujuh) NAP, 22 (dua puluh dua) Penyedia Jasa Internet (PJI/ISP), dan KEMDIKBUD.

2. Metoda

Penyusunan dokumen Dwi Bulanan I 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].

[2] *Fraud*, `http://en.wikipedia.org/wiki/Fraud`
[3] *Malware*, `http://en.wikipedia.org/wiki/Malware`

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.

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

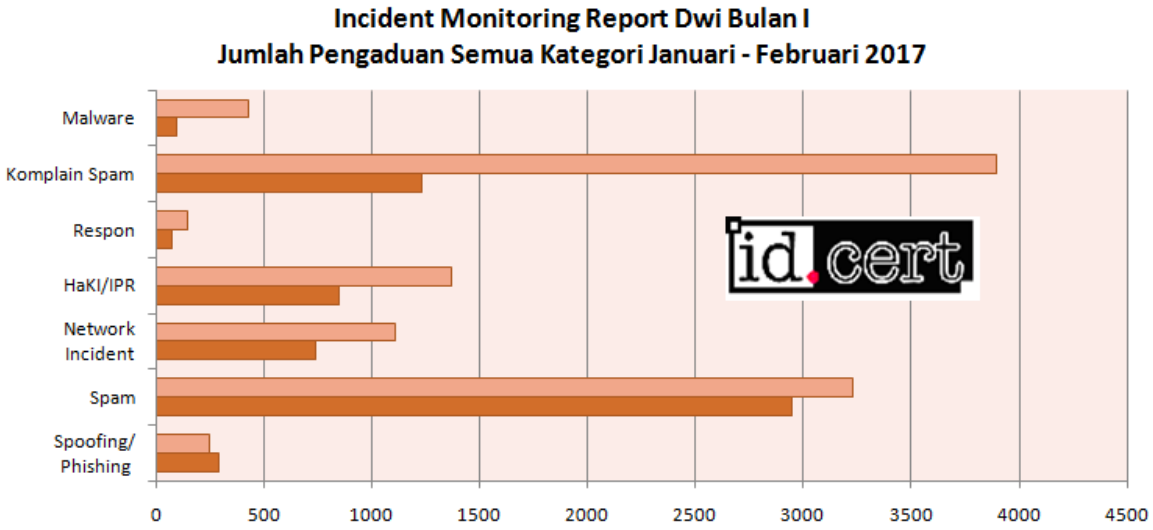
3. Uraian

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



	Spoofing/ Phishing	Spam	Network Incident	HaKI/IPR	Respon	Komplain Spam	Malware
Januari	250	3228	1107	1372	146	3892	433
Februari	293	2948	738	852	76	1235	99

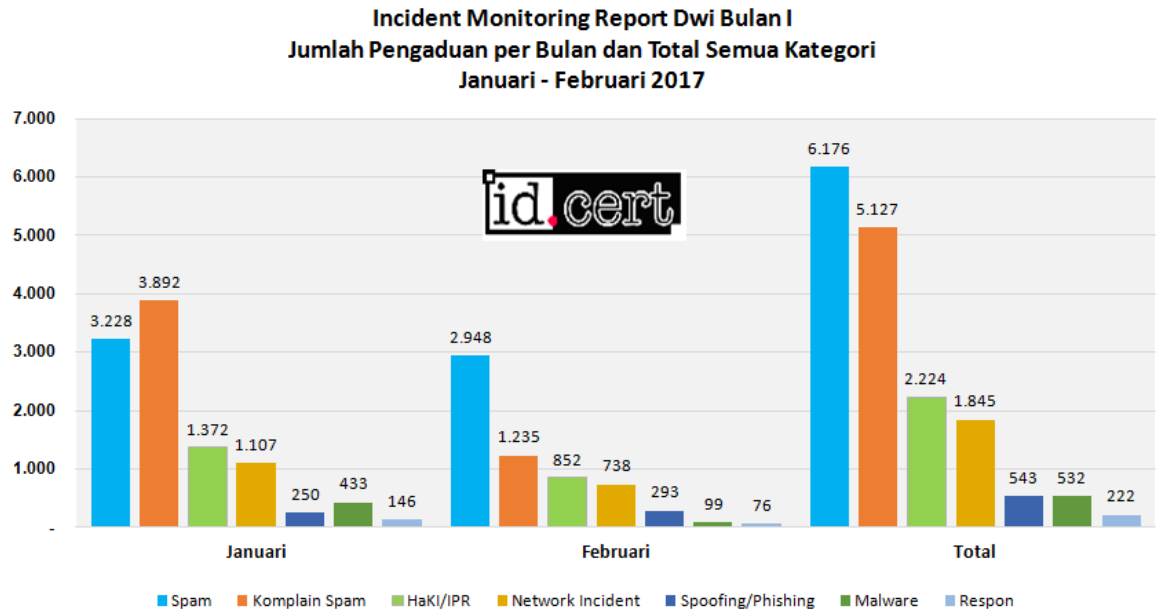
Gambar 1 Jumlah pengaduan semua kategori Januari – Februari 2017

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 Januari – Februari 2017

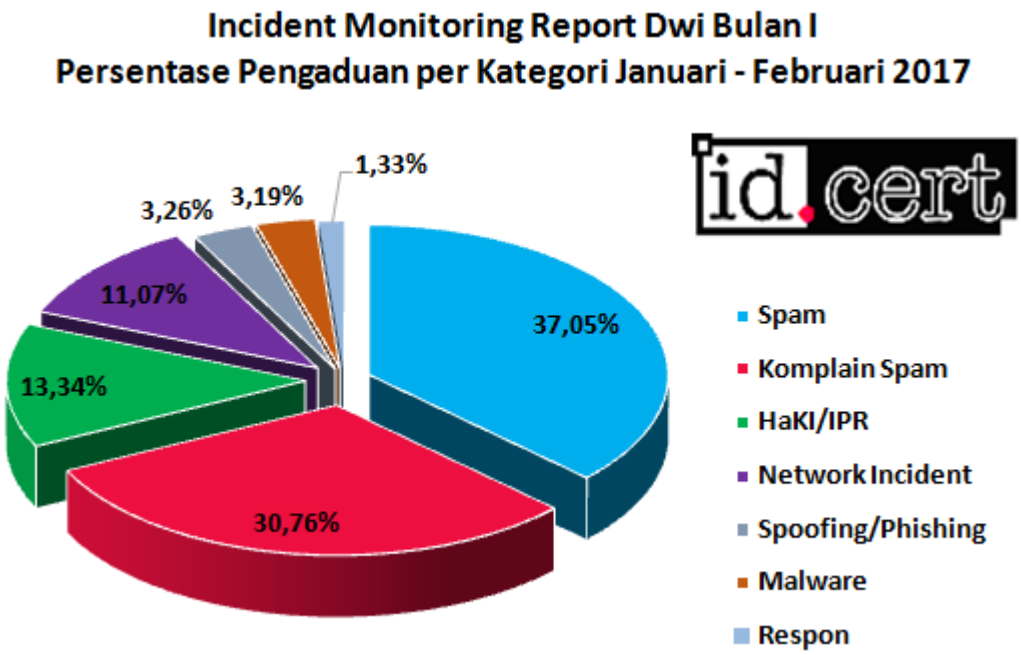
Kategori	Jan	Feb	Total	%
Spam	3.228	2.948	6176	37,05%
Komplain Spam	3.892	1.235	5127	30,76%
HaKI/IPR	1.372	852	2224	13,34%
Network Incident	1.107	738	1845	11,07%
Spoofing/Phishing	250	293	543	3,26%
Malware	433	99	532	3,19%
Respon	146	76	222	1,33%

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



Gambar 2 Jumlah pengaduan per bulan dan total semua kategori Januari – Februari 2017

Perhitungan perkembangan dilakukan terhadap jumlah pengaduan pada bulan pertama Januari, bulan kedua Februari dan bernilai negatif jika terjadi penurunan. Tren untuk Dwi Bulan I ini yaitu hanya satu kategori yang mengalami peningkatan dan sebagian besar kategori mengalami penurunan jumlah pengaduan pada bulan Februari. 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 I 2017

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

Tabel 2 Perkembangan jumlah pengaduan dalam persentase

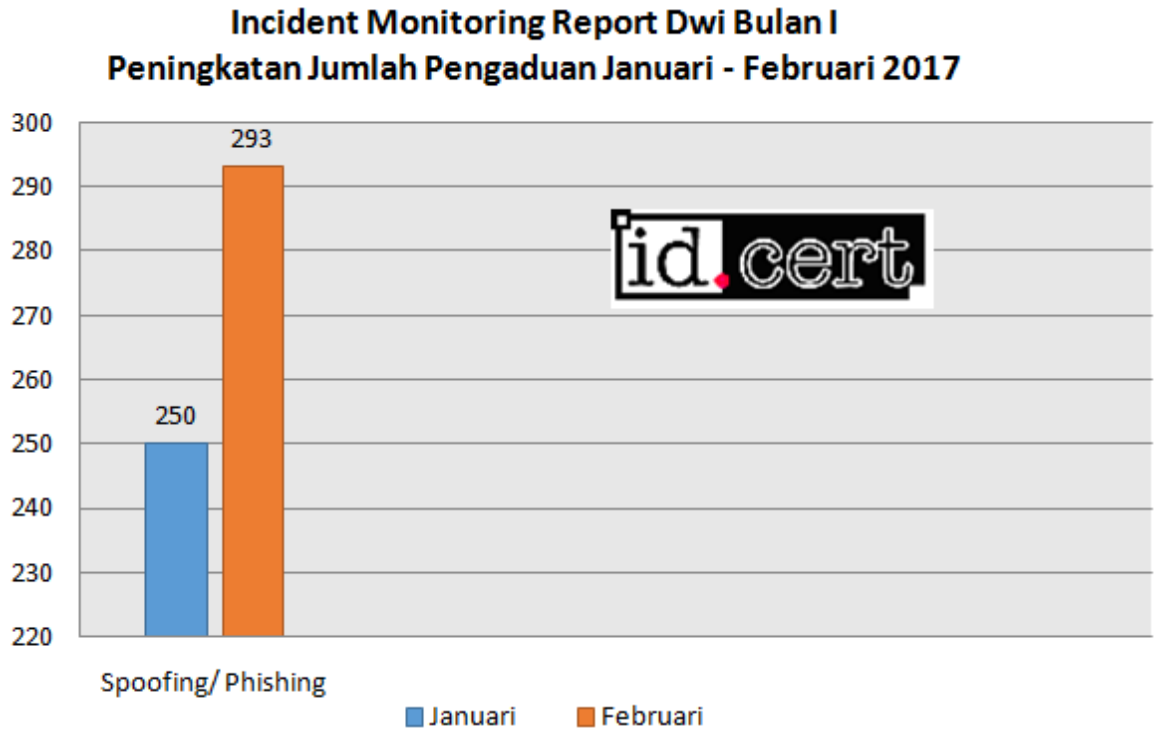
Kategori	Januari	Februari	%
Spoofing/Phishing	250	293	17,20%
Spam	3228	2948	-8,67%
Network Incident	1107	738	-33,33%
HaKI/IPR	1372	852	-37,90%
Respon	146	76	-47,95%
Komplain Spam	3892	1235	-68,27%
Malware	433	99	-77,14%

3.1 Kelompok Pengaduan yang Mengalami Peningkatan

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

1. *Spoofing/Phishing* mengalami peningkatan jumlah pengaduan dari bulan Januari ke Februari, dari 250 meningkat menjadi 293. Persentase peningkatannya mencapai sebesar 17,20%.

Grafik peningkatan pengaduan tersebut disajikan pada Gambar 4.



Gambar 4 Peningkatan Jumlah Pengaduan pada bulan Januari – Februari 2017

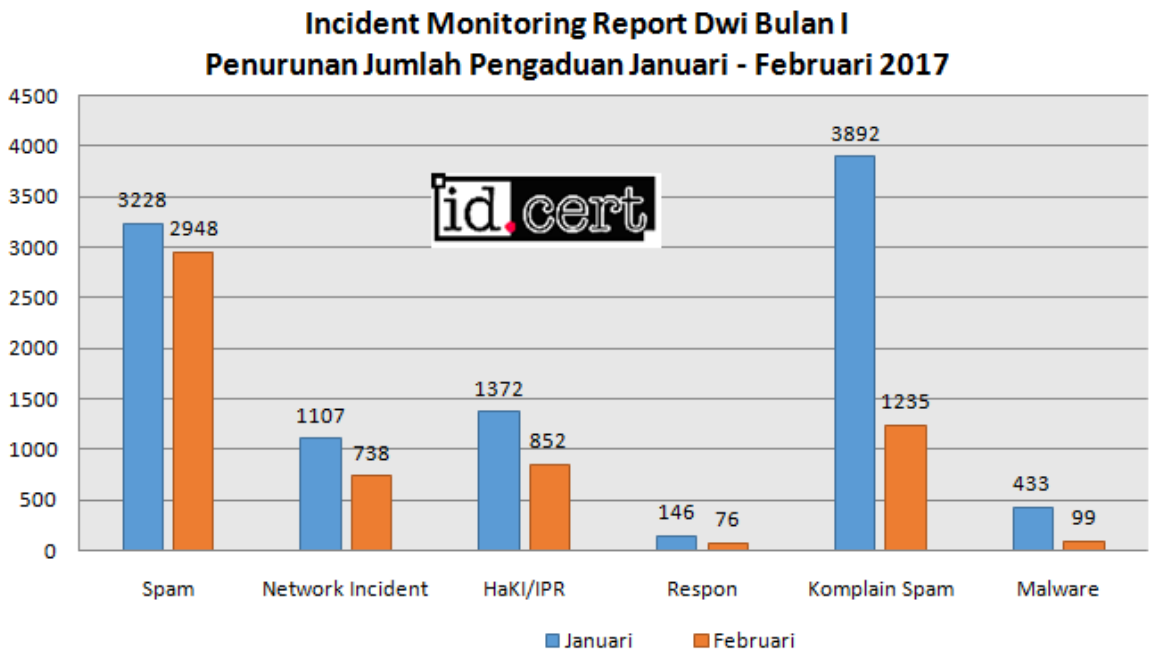
3.2 Kelompok Pengaduan yang Mengalami Penurunan

Bulan Januari – Februari 2017 terdapat kategori yang mengalami penurunan jumlah pengaduan di bulan kedua, yaitu:

1. *Spam* mengalami peningkatan jumlah pengaduan dari 3.228 pada bulan Januari dan turun sebesar 8,67% di bulan Februari dengan jumlah pengaduan sebanyak 2.948.

2. *Network Incident* pada bulan Januari berjumlah 1.107 pengaduan dan menurun sebesar 33,33% di bulan Februari, yaitu dengan jumlah *Network Incident* sebanyak 738 pengaduan.
3. Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR) mengalami penurunan jumlah pengaduan dari bulan Januari ke Februari, dari 1.372 turun ke 852. Persentase penurunannya sebesar 37,90%.
4. Respon juga mengalami penurunan jumlah dari bulan Januari ke Februari ini. Respon memiliki jumlah sebanyak 146 pada bulan Januari dan turun dengan persentase sebesar 47,95% di bulan Februari dengan jumlah sebanyak 76.
5. Komplain Spam memiliki jumlah pengaduan sejumlah 3.892 di bulan Januari. Pada bulan Februari terjadi penurunan jumlah pengaduan dibandingkan dengan bulan Januari dengan persentase penurunan sebesar 68,27% yang berjumlah 1.235 pengaduan.
6. *Malware* mengalami penurunan jumlah pengaduan yang cukup besar bulan Februari. Jumlah pengaduan di bulan Januari sebanyak 433 dan di bulan Februari sebanyak 99. Secara persentase penurunan jumlah pengaduan dari bulan Januari ke Februari mencapai 77,14%.

Grafik penurunan jumlah pengaduan disajikan pada Gambar 5.



Gambar 5 Penurunan Jumlah Pengaduan pada bulan Januari – Februari 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 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