Laporan Dwi Bulan II 2013

ID-CERT[1]

Ringkasan
Di laporan Dua Bulan II 2013 ini disajikan hasil pengumpulan pengaduan selama dua bulan, Maret dan April 2013. Pengaduan tsb. diterima dalam bentuk email dan dikumpulkan sesuai kategori, sebagai bahan penyusunan statistik, dalam bentuk angka dan grafik. *Spam*, komplain *spam*, respon, *network incident*, Hak atas Kekayaan Intelektual, *fraud*, *spoofing*/*phising*, dan *malware* merupakan kategori yang dipilih untuk pengelompokan pengaduan yang masuk.

Kata kunci
Security – Pelaporan – Laporan Dwi Bulan

[1] *Diterbitkan June 6, 2013*

Daftar Isi

1. Pendahuluan

Bagian penting dari kegiatan sekarang ini adalah Internet. Pemakaiannya sehari-hari semakin penting – dari komunikasi antarwarga hingga transaksi bisnis multinasional, pengguna Internet kian banyak dan kian beragam – usia kanak-kanak sampai dengan para lansia, para pekerja di lapangan sampai dengan *bot* otomatis. Batas-batas yang telah ada sebelumnya juga mengalami pergeseran dengan adanya Internet, menciptakan kemungkinan baru yang perlu dicermati. Tidak terkecuali aspek keamanan Internet (*Internet security*) yang menjadi perhatian secara khusus dan kerja sama banyak kalangan.

Sebagai bagian dari pemantauan keamanan Internet, ID-CERT[1] menerima pengaduan lewat email yang diterima dari beberapa responden. Pengaduan tsb. dikelompokkan 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 2013. Selain gambaran tsb., 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

[1] Indonesia Computer Emergency Response Team.

pihak-pihak di mancanegara berkaitan dengan penanganan laporan. Pengaduan yang diterima memberi gambaran bagian-bagian yang perlu dibenahi, keterkaitan antarlembaga, dan untuk membantu penyusunan rencana ke depan.

Pada laporan Dwi Bulanan II 2013, *network incident* masih menempati jumlah pengaduan terbanyak, dengan demikian masih bertengger pada peringkat pertama seperti pada laporan Dwi Bulanan I 2013. Dilihat dari sisi jumlah pengaduan, terdapat tiga kelompok besar: *network incident* sendirian pada kelompok pertama, selanjutnya kelompok kedua memiliki jumlah pelaporan sedang, dan kelompok terakhir berjumlah pengaduan rendah. Penjelasan lengkap tentang ketiga kelompok tsb. dipaparkan di bagian *Uraian*.

Pada penelitian ini, data 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 Interenet (PJI/ISP).

Statistik ini juga mendapat dukungan sponsor dari Pengelola Nama Domain Internet Indonesia (PANDI) dan Asosiasi Penyedia Jasa Internet Indonesia (APJII).

2. Metoda

Penyusunan dokumen Dwi Bulan ini 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 sbb.:

Fraud Penipuan disengaja yang dibuat untuk keuntungan pribadi atau untuk merugikan individu lain[2].

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 pengelolaan pesan elektronik untuk mengirim pesan-pesan tidak-diharapkan dalam jumlah banyak, terutama untuk pengiklanan, tanpa pilih-pilih[4].

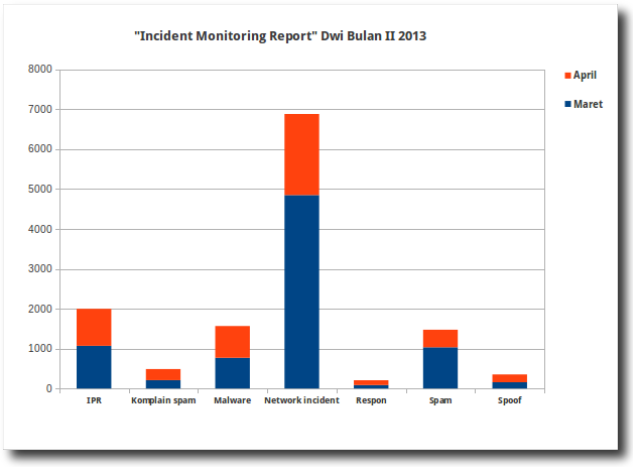
Spoofing/Phishing Pemalsuan email dan situs untuk menipu pengguna[5].

Lain-lain Laporan penyalahgunaan selain yang termasuk pada kategori di atas.

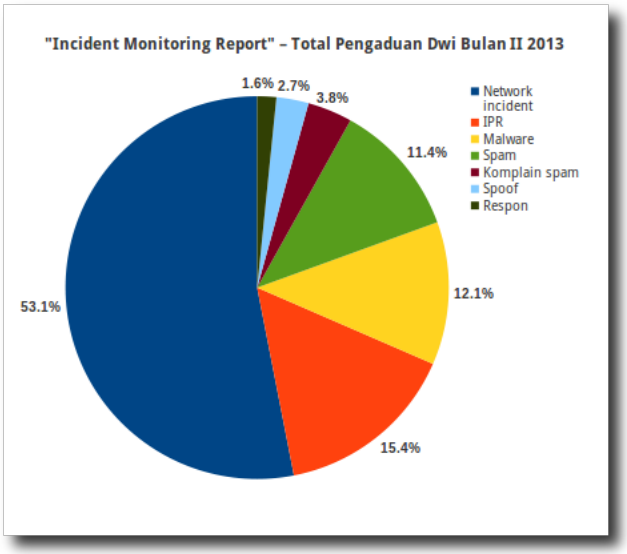
3. Uraian

Email pengaduan yang diterima dikumpulkan berdasarkan topik pelaporan dan bulan, dengan demikian terdapat dua kelompok besar, bulan Maret dan April 2013. Topik pelaporan terdiri atas Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR), komplain spam, *malware*, *network incident*, respon, *spam*, dan *spoof*. Berikut jumlah pengaduan yang diterima ditampilkan dalam bentuk histogram.

[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`



Gambar 1. *Incident Monitoring Report* Dwi Bulan II 2013



Gambar 2. Persentase pengaduan pada Dwi Bulan II 2013

Lebih rinci, jumlah pengaduan masing-masing dapat dilihat dengan lebih seksama pada tabel di bawah ini, diurutkan berdasar abjad jenis pengaduan.

Jenis	Maret	April	Perkembangan
IPR	1070	927	−13,36%
Komplain spam	209	279	33,49%
Malware	771	795	3,11%
Network incident	4850	2032	−58,10%
Respon	86	122	41,86%
Spam	1033	440	−57,41%
Spoof	158	195	23,42%

Table 1. Perkembangan jenis pengaduan dalam dua bulan

Secara umum terjadi penurunan jumlah pelaporan pada bulan April dibanding Maret, *network incident* dan *spam* mengalami penurunan cukup besar, lebih dari separuh. Hanya komplain akan spam yang mengalami peningkatan.

Total pengaduan selama dua bulan dan persentase masing-masing dapat dilihat pada tabel dan grafik berikut ini.

Jenis	Maret	April	Total	Persentase
Network incident	4850	2032	6882	53,1%
IPR	1070	927	1997	15,4%
Malware	771	795	1566	12,1%
Spam	1033	440	1473	11,4%
Komplain spam	209	279	488	3,8%
Spoof	158	195	353	2,7%
Respon	86	122	208	1,6%

Table 2. Persentase jenis pengaduan

3.1 *Network Incident* pada posisi tertinggi

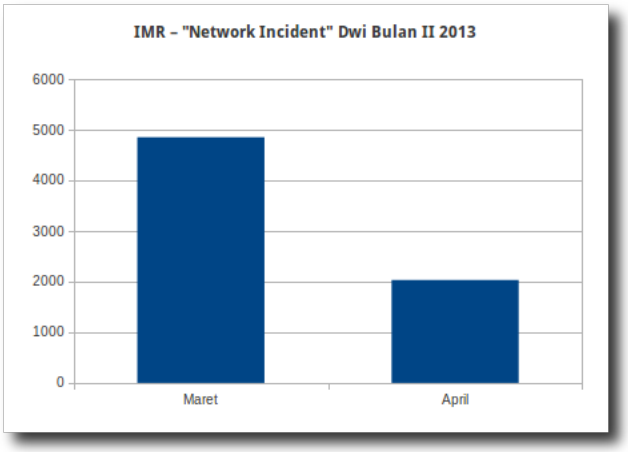
Network incident menempati posisi tertinggi, berjumlah total 6.800-lebih email yang diterima. Dari email tsb., pengaduan paling banyak berupa gangguan ke Postfix[6], berjumlah 6129 laporan atau 90% dari keseluruhan. Laporan gangguan terbanyak ini berasal dari satu sumber di mancanegara. Mayoritas pelaporan sejumlah alamat IP yang berbeda-beda yang dimiliki salah satu PJI/ISP[7], sehingga kemungkinan besar insiden ini diawali dari komputer klien PJI tsb.

Terjadi penurunan signifikan pada pelaporan *network incident* pada periode kedua, April 2013, hingga -58%, sedangkan secara keseluruhan peringkat teratas *network incident* ini jauh lebih banyak daripada jenis pelaporan lainnya.

Pada Gambar 3 ditampilkan contoh email pengaduan *network incident*, yang dihasilkan secara otomatis oleh sistem dan dikirimkan ke PJI yang menangani asal gangguan.

[6]Postfix adalah perangkat lunak server email atau dikenal dengan *Mail Transfer Agent* (MTA) dan berdasarkan perhitungan tahun 2012 disebut digunakan oleh 23% server email di Internet. Sumber: Wikipedia, `http://en.wikipedia.org/wiki/Postfix_(software)`

[7]Penyelenggara Jasa Internet (*Internet Service Provider*)



Gambar 3. *Network incident*

3.2 Bagian 2: *IPR*, *Malware*, dan *Spam*

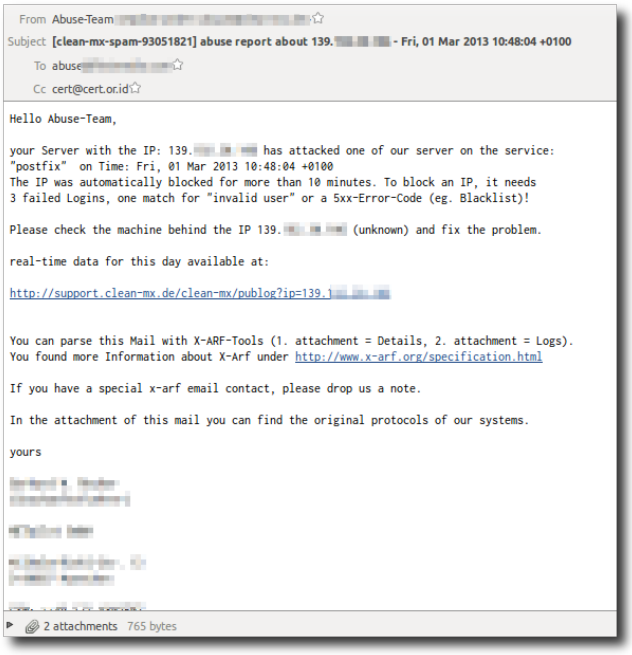
Pada Bagian 2 pelaporan, yang diisi IPR, *malware*, dan *spam* pelaporan masing-masing berkisar pada angka 1500 hingga 2000, dengan demikian bagian ini dapat disebut sebagai "grup dua ribuan".

Jauh di bawah *network incident*, *Intellectual Property Right* (IPR) atau Hak atas Kekayaan Intelektual (HaKI) berada pada peringkat kedua dari jumlah laporan yang masuk, sekitar 2.000 laporan, atau pada kisaran 15% dari keseluruhan. IPR juga mengalami penurunan pada periode kedua, sebesar -13%, menjadikan jumlah pelaporan cukup seimbang pada dua bulan tsb.

Contoh email pengaduan kasus IPR ditunjukkan di Gambar 4.

Malware berada pada peringkat ketiga, dengan pengaduan sekitar 1500 laporan dan pada kelompok ini – berbeda dengan yang lain – mengalami peningkatan, sebesar 3%, menghasilkan "bentuk yang merata" selama dua bulan. Dari pengaduan yang masuk, terdapat serangkaian DDOS-Malware dan Fast Flux.

Spam berada pada peringkat keempat, dengan jumlah pengaduan sekitar 1400 laporan atau 11% dari total laporan. Pada periode ini, spam mengalami penurunan tajam pada bulan kedua, sebesar -57,4%, berada pada peringkat kedua, setelah *network incident*.


From Abuse-Team
Subject [clean-mx-spam-93051821] abuse report about 139. - Fri, 01 Mar 2013 10:48:04 +0100
To abuse
Cc cert@cert.or.id

Hello Abuse-Team,

your Server with the IP: 139. has attacked one of our server on the service:
"postfix" on Time: Fri, 01 Mar 2013 10:48:04 +0100
The IP was automatically blocked for more than 10 minutes. To block an IP, it needs
3 failed Logins, one match for "invalid user" or a 5xx-Error-Code (eg. Blacklist)!

Please check the machine behind the IP 139. (unknown) and fix the problem.

real-time data for this day available at:

http://support.clean-mx.de/clean-mx/publog?ip=139.

You can parse this Mail with X-ARF-Tools (1. attachment = Details, 2. attachment = Logs).
You found more Information about X-Arf under http://www.x-arf.org/specification.html

If you have a special x-arf email contact, please drop us a note.

In the attachment of this mail you can find the original protocols of our systems.

yours

2 attachments 765 bytes

Gambar 4. Contoh pengaduan *network incident* lewat email

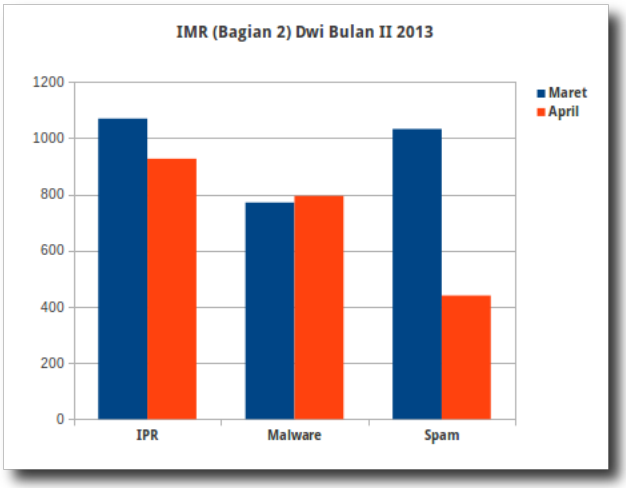
3.3 Bagian 3: Komplain *Spam*, *Spoof*, dan Respon

Pada Bagian 3 pelaporan, yang diisi komplain *spam*, *spoof*, dan respon, pelaporan masing-masing berkisar pada angka 500, dengan demikian bagian ini dapat disebut sebagai "grup lima ratusan".

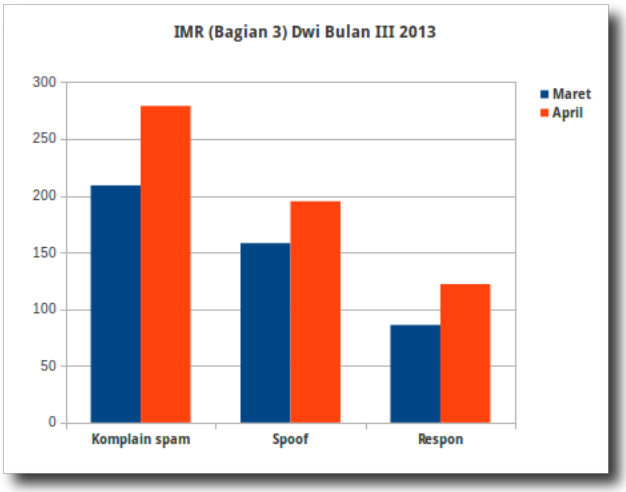
Jika laporan aktivitas *spam* secara umum dihasilkan secara otomatis oleh sistem *anti-spam*, "komplain *spam*" merupakan laporan atas gangguan *spam*, sehingga terlihat bersifat insidental dan berjumlah sedikit, yakni jika pengguna merasa perlu melaporkan. Pada periode ini jumlah laporan komplain-spam sebesar 4%, dengan peningkatan jumlah pelaporan sebesar 33% dari Maret ke April.

Dari beberapa kemungkinan fenomena ini, dua poin perlu dipertimbangkan:

1. Media pelaporan seperti IDCERT tidak dipertimbangkan oleh penerima *spam*.
2. 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



Gambar 5. Grafik IPR, *Malware*, dan Spam



Gambar 6. Komplain *Spam*, *Spoof*, dan Respon

spam ini dengan cukup menghapusnya.

Jumlah pengaduan *spoof* sebesar 3% dari total pelaporan dan pada periode ini mengalami peningkatan sebesar 23%, sedangkan untuk respon sebesar 2% dari total pelaporan dan mengalami peningkatan sebesar 42%.

4. Rangkuman

Dengan pertimbangan jumlah gangguan berupa *network incident* yang masih teratas, perlu menjadi perhatian para administrator jaringan, baik untuk jaringan lokal atau jaringan di bawah layanan Penyedia Jasa Internet (PJI), agar mempertimbangkan tindakan preventif mengurangi penyalahgunaan akses keluar dari pengguna di dalam jaringan. Hal ini sesuai dengan pendapat sebagian ahli keamanan jaringan bahwa “gangguan dapat muncul dari dalam, pengguna jaringan itu sendiri”, baik dilakukan dengan sengaja atau ketidaksengajaan seperti penyusupan *bot* di komputer.

Dilihat dari volume pengaduan yang masuk – yang menggambarkan kepedulian para pelapor terhadap isu keamanan Internet – menjadi tanggung jawab pihak-pihak terkait dengan bahan laporan tsb. 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 virus dan perangkat lunak keamanan dipasang untuk mengurangi risiko terinfeksi *malware*. Pemutakhiran terhadap aplikasi dan basis data yang terkait dengan aplikasi dilakukan secara teratur.
2. Administrator jaringan perlu melakukan pemantauan terhadap aksi yang mencurigakan, semisal akses ke *port* email/Postfix[8] secara intensif dalam periode lama atau berulang-ulang.
3. Administrator jaringan memblokir semua *port* akses ke Internet, kecuali untuk *port* yang dianggap diperlukan.
4. Penyedia Jasa Internet (PJI/ISP) dan operator telekomunikasi disarankan menyediakan tombol pelaporan khusus penyalahgunaan Internet (*Internet abuse*) guna kemudahan pelaporan.
5. Formulir pengaduan penyalahgunaan Internet (*Internet abuse*) dicantumkan di setiap situs web.
6. Terkait Hak atas Kekayaan Intelektual (HaKI), sebaiknya pemerintah menyiapkan aturan hukum yang

[8] Terkait jumlah pengaduan *network incident* yang sangat banyak.

jelas mengenai materi (*content*) yang dianggap melanggar HaKI, karena PJI atau penyedia materi memerlukan landasan hukum yang jelas untuk menurunkan materi yang bermasalah.

7. Semua pihak wajib menindaklanjuti setiap laporan keluhan/pengaduan yang diterimanya. Bila menyangkut pelanggaran hukum, sebaiknya dilaporkan kepada penegak hukum.

5. Ucapan terima kasih

Terima kasih pada seluruh responden yang telah berpartisipasi pada pengumpulan bahan untuk penulisan laporan ID-CERT, yakni:

1. Kementrian Komunikasi dan Informatika (Kominfo).
2. Pengelola Nama Domain Internet Indonesia (PANDI).
3. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII).
4. Detik (Detik.net).
5. Tiga operator telekomunikasi, tujuh NAP, dan dua puluh dua PJI/ISP.

6. Lampiran

6.1 Penipuan di Ranah Maya

Penipuan lewat media daring (*online media*) merupakan topik hangat pada periode Maret-April 2013. Dibicarakan di media sosial dan menjadi perhatian sejumlah media massa. Pesan tentang penipuan lewat media daring ini juga datang sebagai berikut,

> Salam hormat.
>
> Saya praktisi internet di Cilacap, teringat kejadian pada tahun 2012, www.***.com yang di-*hosting* di **** menjadi geger di Cilacap, karena ada pembeli yang komplain sudah transfer ke pemilik, ternyata toko *online* tersebut adalah palsu, dan dari dinas Dishubkominfo Cilacap menghubungi pihak **** untuk memproses domain tersebut, minimal mematikannya, dan memang dalam hitungan minggu domain tersebut tutup.
>
> Kenyataannya masih banyak penipu *online* yang menggunakan *hosting* dari ****, contohnya: a***.com, m***.com, m***.com, f****.com, dsb. Alangkah baiknya jika pihak **** juga ikut membantu secara proaktif untuk membatasi menjamurnya situs penipu ini dengan memverifikasi ulang situs-situs *ecommerce* yang ada di ****, jangan hanya mengejar penjualan semata.
>
> Seharusnya penipuan *online* pun juga bisa dilakukan tindak lanjut preventif dari pihak *hosting* dan ada tindakan penghukuman dengan disediakannya jalur untuk masyarakat mengadu secara *online* dan pihak kepolisian dan kejaksaan diharapkan ikut membantu jika memang terjadi penipuan.
>
> Intinya adalah bagaimana caranya membuat ruang gerak para penipu *online* ini juga jera, dan merasa semua usaha mereka terbatasi. Mereka sudah susah uang habis buat domain, setelah diproses di tempat *hosting* lokal dan beberapa minggu diawasi, ternyata *scam*/penipu, maka *hosting* berhak menutup otomatis, jika ada insiden, di-*hosting* di luar, pihak nawala juga ikut memblokir sehingga tidak ada korban lainnya, sementara polisi dan kejaksaan menindaklanjuti dari segi hukumnya.
>
> Untuk kepedulian dalam usaha menciptakan internet yang sehat, aman, dan terpercaya, saya ucapkan terima kasih

Sebagai respon terhadap email di atas, dilakukan diskusi di *mailing list*, dan disampaikan poin-poin sebagai usulan sbb.

1. Menyelenggarakan sosialisasi lebih sering. Pengetahuan untuk konsumen menjadi bagian paling penting dan relatif lebih mudah dikerjakan oleh semua pihak yang peduli masalah ini. Sosialisasi dapat dilakukan dalam bentuk ekspos ke masyarakat, seperti pameran, seminar, tulisan-tulisan di media sosial. Agar berlangsung dengan lebih baik, dapat diorganisasi bersama komunitas lain yang berkepentingan. Tindakan ini preventif dan tidak mengarah ke sanksi terhadap pelaku, namun lebih mudah dilakukan oleh semua pihak. Tujuan akhirnya: kesadaran pengguna Net atau calon konsumen meningkat.
2. Menyediakan organisasi pemantau (*watch*). Organisasi pemantau ini menyediakan media untuk pelaporan masyarakat, mengelola basis data pelaporan, dan mendistribusikan hasil pelaporan dan keputusan organisasi ke perangkat yang dapat membantu mengurangi peluang kejahatan, seperti tempat hosting penipu, layanan DNS seperti Nawala Nusantara[9] dan OpenDNS[10].
3. Mengusulkan pembentukan badan akreditasi resmi.

[9] *Nawala Nusantara*, `http://nawala.org`
[10] *OpenDNS*, `http://opendns.com`

Badan akreditasi menyelenggarakan sertifikasi resmi dengan cara praktis dan terjangkau, sehingga tidak menyulitkan orang yang benar-benar menyelenggarakan bisnis *online*, namun tetap kredibel terkait keputusan suatu status dapat dipercaya atau belum. Tata cara akreditasi dibahas lebih rinci oleh badan.

4. Menyiapkan alur kerja (*workflow*).
   Alur kerja ini berisi dari pemantauan atau pelaporan hingga berupa keputusan yang digunakan bersama untuk koordinasi antarinstansi.

Urutan 1 s.d. 4 di atas sesuai tingkat kesulitan: bagian pertama (1) paling mudah dilakukan.

Untuk sosialisasi, ini juga sempat dibicarakan dengan Direktorat Keamanan dan Informasi (DKI), Kementerian Komunikasi dan Informatika (Kominfo), saat rapat dengan sejumlah CSIRT di Indonesia seminggu lalu. Direktorat berharap ID-CERT selaku CERT publik bisa lebih memberikan sosialisasi penanganan insiden beserta contoh-contoh kasusnya secara lebih spesifik, sehingga hal ini dapat mengedukasi publik.

Dari diskusi pula disampaikan artikel di Detikinet, tentang artikel berisi inisiatif mengumpulkan senarai toko daring palsu, *Catat! Ini Daftar Toko Online Abal-abal*[11].

[11] URL: http://goo.gl/EVLZe (Detikinet).