Laporan Kegiatan ID-CERT 2012
Daftar Isi

LAPORAN AKTIFITAS

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM TAHUN 2012

Edisi: 30 Nop 2012

1 Mengenai ID-CERT

1.1 Abstrak

CERT (Computer Emergency Response Team) merupakan tim koordinasi teknis terkait insiden jaringan internet di seluruh dunia. Belakangan tim ini disempurnakan lagi melalui RFC 2350 dengan nama CSIRT (Computer Security Incident Response Team).

CERT maupun CSIRT di setiap negara umumnya dibangun oleh komunitas. Walaupun ada juga yang didukung oleh negara seperti halnya KrCERT (Korea Selatan), JPCERT (Jepang), AusCERT (Australia), dsb.

Yang juga perlu disadari: CERT di setiap negara memiliki beragam kewenangan pekerjaan dan konstituen yang digarap. Beberapa CERT memiliki pola yang sedikit berbeda di satu negara dengan negara lainnya. Misalnya CERT di Korea Selatan yang memiliki kewenangan hingga pada persoalan keamanan sibernetika nasional; sedangkan CERT Australia memiliki konstituen dan anggota sehingga dari keadaan tersebut mereka dapat membiayai kegiatan.

Dan adapula CERT/CSIRT yang dibangun oleh komunitas terbatas ataupun negara dengan ruang lingkup yang terbatas untuk kalangan tertutup, seperti MilCERT (Militer), GovCERT (Institusi Pemerintah), BankingCERT (perbankan), ISPCERT (ISP) dan lain sebagainya.

CERT/CSIRT juga melakukan koordinasi di dalam suatu negara (baik dengan sesama CERT/CSIRT maupun organisasi lainnya) dan juga lintas negara. Seringkali antar CERT/CSIRT melakukan koordinasi bila melibatkan insiden jaringan internet. Hubungan yang baik perlu dibangun antar CERT/CSIRT, diantaranya melalui sebuah forum regional yang bernama APCERT (Asia Pacific CERT) yang dibangun oleh seluruh CERT di Asia Pasifik termasuk ID-CERT sebagai salah satu pendirinya.

1.2 Pendahuluan

ID-CERT atau Indonesia Computer Emergency Response Team merupakan sebuah Tim CERT pertama yang berdiri di Indonesia pada 1997. ID-CERT merupakan sebuah tim koordinasi teknis berbasis komunitas dan untuk komunitas yang bersifat independen.

Didirikan oleh Bpk. DR. Budi Rahardjo, ID-CERT bersama dengan JP-CERT (Jepang) dan AusCERT (Australia) merupakan salah satu pendiri dari forum APCERT (Asia Pacific Computer Emergency Response Team).

Peran ID-CERT yang ada selama ini melakukan fungsi koordinasi teknis terhadap komplain yang diterima dan bersifat reaktif, baik di dalam negeri maupun ke luar negeri.

1.3 Pembentukan

Pembentukan ID-CERT diawali dengan "nekat", berdasarkan pertimbangan belum adanya CERT di Indonesia pada saat itu, tahun 1997. Dengan bentuk yang informal dan yang penting didaftarkan terlebih dulu, maka terbentuklah ID-CERT. Pada saat tersebut negara-negara di sekitar Indonesia juga mulai mengupayakan CERT dan hal ini berlanjut ke forum Asia-Pasifik, yang kemudian menjadi cikal-bakal APCERT.

Pertemuan APCERT pertama dihadiri oleh DR. Budi Rahardjo dan Andika Triwidada, di Tokyo, Jepang, pada tahun 2001. Pertemuan APCERT menjadi agenda rutin tahunan yang dilangsungkan secara bergilir di antara anggotanya. Dua negara yang paling aktif di APCERT adalah Australia dan Jepang.

Kendala dari ID-CERT untuk menghadiri acara rutin APCERT adalah pendanaan, yang hingga hari ini

belum dapat swadaya.

Dari sisi organisasi, ID-CERT ingin tetap berdiri sebagai organisasi non-pemerintah, independen, namun mendapat alokasi pendanaan dari pemerintah sebagai kontribusi terhadap CERT.

Dengan bentuk yang sekarang ID-CERT bersikap reaktif (bukan aktif) terhadap sebuah kasus yang masuk atau dilaporkan oleh pihak lain. ID-CERT juga tidak memiliki kewenangan untuk menyelidiki sebuah kasus secara/hingga tuntas, melainkan hanya menjadi penghubung yang dapat dipercaya, terutama oleh pihak yang melaporkan adanya insiden.

1.4 Misi dan Tujuan

1. ID-CERT tidak memiliki otoritas secara operasional terhadap konstituensinya baik di Indonesia maupun luar negeri, melainkan hanya menginformasikan berbagai keluhan atas insiden jaringan, serta bergantung sepenuhnya pada kerjasama dengan para pihak yang terlibat dalam insiden jaringan terkait.
2. ID-CERT dibangun oleh komunitas dan hasilnya akan kembali kepada komunitas.
3. Memasyarakatkan pentingnya keamanan internet di Indonesia.
4. Melakukan berbagai penelitian di bidang keamanan internet yang dibutuhkan oleh komunitas internet Indonesia.
5. Tujuan ID-CERT adalah untuk melakukan koordinasi penanganan insiden yang melibatkan pihak Indonesia dan luar negeri

1.5 Personil

Sejak awal pembentukannya, ID-CERT diketuai oleh Bapak Budi Rahardjo,PhD dan Wakil Ketua Bapak Andika Triwidada.

Dalam aktifitas operasional ID-CERT, beliau dibantu oleh sejumlah staf profesional dan juga voluntir.

1.6 Konstituensi

Konstituen / anggota ID-CERT adalah organisasi umum dan bersifat terbuka.

2 Aktifitas dan Operasional

2.1 Aktivitas

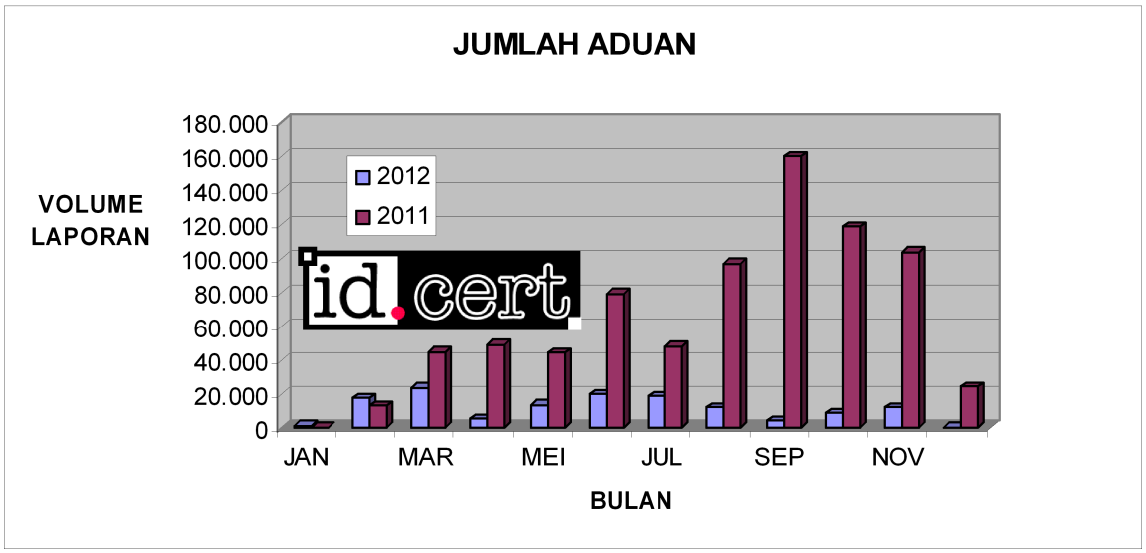
ID-CERT bersikap reaktif, yakni melakukan pekerjaan berdasarkan masukan dari pihak luar, dalam hal ini melalui pelaporan yang diterimanya.

Dari sekian banyak email yang masuk ke ID-CERT sendiri, insiden "phishing" merupakan laporan yang paling banyak diterima. Laporan ini diterima secara perorangan -- umumnya diterima oleh DR. Budi Rahardjo, Andika Triwidada, dan Ahmad Alkazimy -- yang kemudian diteruskan ke situs yang dilaporkan bermasalah atau ke penyedia layanan yang bersangkutan. Selain itu, media lain yang digunakan untuk memaparkan kasus dan perkembangannya adalah milis.

Kini ID-CERT telah memiliki sebuah "helpdesk" yang mengelola pesan kedatangan laporan dan perkembangan penyelesaiannya. Saat ini, ID-CERT dijalankan oleh para profesional dan didukung oleh para voluntir. Tuntutan akan "helpdesk" ini berkaitan pelayanan dan penanganan komplain insiden, juga dengan keperluan menampilkan statistik kasus yang ditangani, yang selalu dipresentasikan di pertemuan APCERT.

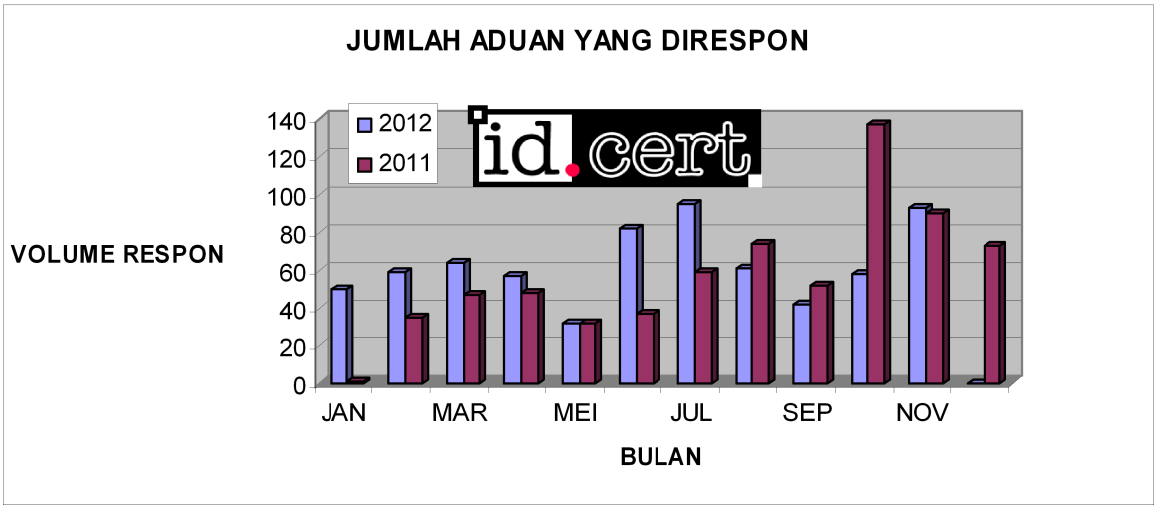
2.1.1 Incident Handling

Saat ini, ID-CERT telah menerima aduan insiden hingga 30 Nop 2012 sebanyak **134.688** aduan insiden sepanjang tahun 2012.



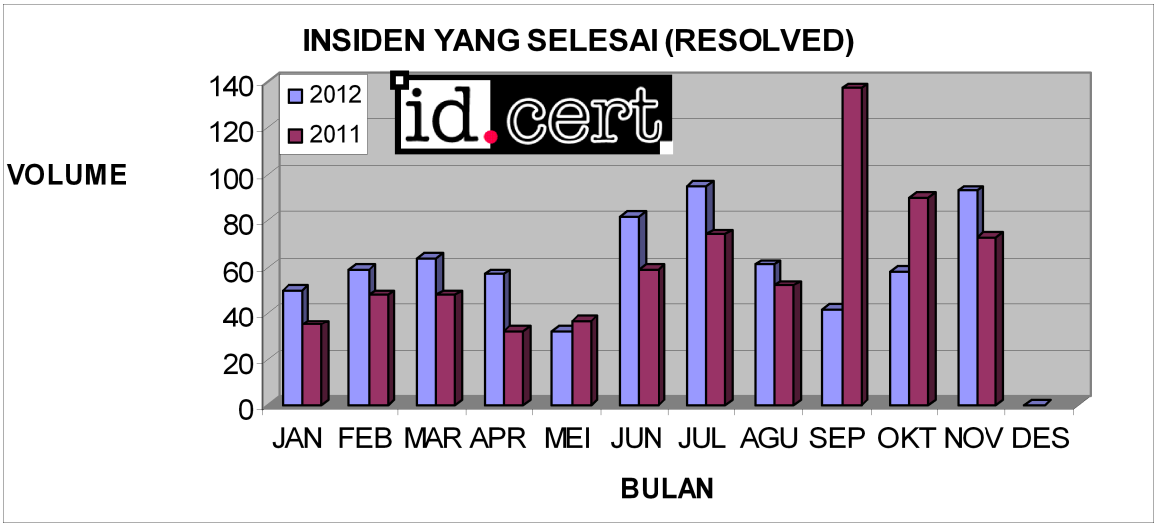
Adapun penanganan aduan dan penyelesaian aduan ditahun 2012 yang kami proses adalah sebanyak 693 insiden. Sedangkan pada tahun 2011 adalah sebanyak 685 insiden yang telah berhasil kami tangani dan kami selesaikan.

Sedangkan tahun 2011, ID-CERT menerima sebanyak **783.457** aduan insiden,



Kami juga telah membuat Standard Operation and Procedures (SOP) terkait penanganan insiden ini dimana aduan yang kami tangani secara **prioritas** adalah aduan yang datang dari dalam negeri serta aduan luar negeri yang merupakan permintaan bantuan ataupun masalah Phishing/Spoofing. Sedangkan aduan insiden yang berupa tembusan (sudah ditujukan ke ISP secara langsung), tidak kami proses lebih lanjut.

Terhitung mulai **01 Nop 2012**, ID-CERT menangani secara penuh seluruh insiden sesuai SOP yang ada dimana sebelumnya, kami hanya fokus pada aduan Phishing/Spoofing serta aduan instansi Pemerintahan saja.



Guna memperlancar penanganan dan proses dokumentasi aduan insiden, efektif pada 01 Nop 2012 ini ID-CERT telah berhasil mengoperasionalkan sistem dokumentasi dan tiket email.

2.1.2 Incident Monitoring Report

Incident Monitoring Report merupakan aktifitas monitoring bersama yang melibatkan peran serta aktif konstituen ID-CERT berupa tembusan email aduan insiden.

ID-CERT dalam 2 tahun terakhir telah melakukan Riset yang terkait dengan penanganan insiden berbasis pengaduan atau yang disebut Incident Monitoring Report dengan melibatkan ISP, NAP, Operator Telekomunikasi serta lembaga non-ISP seperti: Lembaga Pemerintahan dan perusahaan. Dimulai dengan status Riset Internet Abuse pada tahun 2010 dimana ID-CERT menjadi salah satu pendukung riset tersebut.

Kini, terhitung mulai bulan Mar 2012, riset ini telah menjadi salah satu aktivitas rutin ID-CERT yang permanen yang diharapkan dapat berkelanjutan, agar Indonesia dapat memiliki data primer atas Incident Monitoring Report yang terjadi di Indonesia.

Berbeda dengan laporan yang masuk ke ID-CERT di atas, laporan yang masuk melalui riset Internet Abuse sepanjang tahun 2010, bila dirata-rata dengan jumlah laporan komplain yang masuk sebesar 290.297 laporan per bulannya.

Adapun jumlah laporan yang masuk sepanjang tahun 2011 adalah sebanyak **1.057.333** laporan per tahun atau **88.111** laporan rata-rata per bulan:

2011

No.	Kategori	Rating (%)
1	Network Incident	51,48
2	Spam	36,07
3	INTELLECTUAL PROPERTY RIGHTS/HaKI	9,29
4	Malware	3,05
5	Spoofing / Phishing	0,05
6	Respon	0,05
7	Spam Komplain	0,01

2010

NO.	KATEGORI	RATING (%)
1	SPAM	90,83
2	INTELLECTUAL PROPERTY RIGHTS/HaKI	5,41
3	MALWARE	1,95
4	NETWORK INCIDENT	1,74
5	SPOOFING/PHISHING	0,05
6	SPAM KOMPLAIN	0,01
7	RESPON	0,001

Sedangkan untuk tahun 2012, jumlah laporan yang masuk hingga 30 Nop 2012 adalah sebanyak **247.119** laporan.

Kasus yang masuk juga umumnya justru berasal dari manca negara, setelah yang bersangkutan kesulitan menghubungi pengelola situs yang dianggap bermasalah. ID-CERT menjadi pihak yang dapat dipercaya untuk pelaporan kasus tersebut, lebih-lebih dari CERT negara-negara tetangga yang memang telah menjalin hubungan baik, hingga dilakukan kunjungan ke ID-CERT langsung.

2.1.3 Layanan Terbaru

Pada tahun 2012 ini ID-CERT telah meluncurkan sejumlah layanan terbaru, diantaranya adalah:

2.1.3.1 Statistik Malware Indonesia

ID-CERT berencana membuat Statistik tentang Malware yang beredar di Indonesia. Laboratorium ini dimaksudkan untuk mengetahui secara langsung dampak dan kewaspadaan masyarakat internet Indonesia terhadap virus/worm/malware.

Metodologi yang digunakan adalah:

1. Melakukan survey lapangan menggunakan USB Flashdisk yang telah diisi portable apps (aplikasi antivirus yang ada yang ketika dicolokkan ke komputer, tidak perlu lagi melakukan instalasi namun bisa langsung digunakan untuk melakukan scanning PC hingga jaringan).
2. Setelah didapat, maka tim kami akan melakukan pencatatan waktu, nama varian virus serta lokasi penemuannya. Selanjutnya nama-nama virus tersebut akan dimasukkan kedalam database dan dibuatkan statistiknya. Metode pencatatan juga akan dikembangkan agar bisa melakukan *parsing* laporan secara otomatis.
3. Cara yang lain adalah dengan menggunakan sebuah server *honeypots* untuk mengkoleksi berbagai malware yang beredar di Indonesia.

2.1.3.2 Antispam RBL

Antispam RBL merupakan salah satu tools diinternet untuk meminimalisir peredaran Spam.

Pada bulan Juni 2012, ID-CERT telah berhasil melakukan instalasi Antispam RBL yang dibangun khusus atas permintaan APJII. Rencananya pihak APJII akan meluncurkan operasional Antispam RBL Indonesia yang merupakan wujud dari kerjasama ID-CERT dan APJII.

2.1.3.3 Peringatan Keamanan / Security Advisory

Terhitung mulai Nopember 2012, atas saran dari sejumlah CERT sehubungan dengan terjadinya Outbreak Malware Grumbot, maka ID-CERT mulai menerbitkan peringatan dalam format Security Advisory.

Hal ini merupakan pencapaian terbaru ID-CERT setelah selama ini kami mencoba mencari format yang tepat dan jenis Peringatan Keamanan yang cocok bagi konstituen kami. Hingga Des 2012, ID-CERT telah menerbitkan 3 Peringatan Keamanan.

Pada Selasa, 11 Desember 2012, ID-CERT mulai melakukan ujicoba penerbitan Vurnerability Notice (bekerjasama dengan PT SPENTERA) terkait dengan bug yang ditemukan pada sejumlah aplikasi yang ada. Dalam tahap ujicoba ini, ID-CERT akan mempelajari dan mencoba menjadi fasilitator bagi pengembang aplikasi dalam menginformasikan berbagai masalah IT Security.

2.1.3.4 Kontak Desk

Pada 01 Juni 2012, ID-CERT telah meluncurkan nomer kontak baru untuk aduan via telpon, yaitu: **0889-1400-700**.

Adapun untuk aduan umum via email yang selama ini telah berjalan adalah <cert@cert.or.id>.

2.1.4 Kerjasama dengan Organisasi di Dalam Negeri

ID-CERT telah menjalin kerjasama dengan berbagai pihak didalam negeri diantaranya dengan APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), PANDI (Pengelola Nama Domain Indonesia), Direktorat Keamanan Informasi – Kementrian Komunikasi dan Informatika, Direktorat Pengamanan Perdagangan – Kementrian Perdagangan, PT. Arsen Kusuma Indonesia, PT Qwords Company International, PT. SPENTERA, serta berbagai instansi lainnya baik pemerintah maupun swasta.

Pada tahun ini, ID-CERT juga telah menjalin hubungan koordinasi dengan CSIRT lainnya yang ada di Indonesia yaitu: Academic CSIRT dan GovCSIRT.

2.1.5 Kerjasama dengan Organisasi di Luar Negeri

ID-CERT juga telah menjalin hubungan baik dengan anggota APCERT. Selain itu, ID-CERT kini juga telah menjalin hubungan baik dengan sejumlah CSIRT diregional lainnya - terima kasih kepada APCERT atas perkenalannya, penyelenggara antispam RBL, penyelenggara konten, penyelenggara media sosial, serta komunitas anti phishing dan anti spam global.

2.2 Operasional

Terhitung mulai 01 Januari 2012, ID-CERT telah menambah staf Incident Response Officer – Helpdesk untuk menangani masalah aduan insiden, yaitu Sdri. Rahmadian L. Arbianita.

Kini jumlah staf ID-CERT berjumlah 2 (dua) orang. Adapun dalam aktifitas operasionalnya, ID-CERT juga didukung oleh sejumlah voluntir lainnya.

3 Kegiatan

Sejumlah kegiatan telah dilaksanakan oleh ID-CERT, sekalipun dengan keterbatasan dana dan SDM yang kami miliki.

3.1 Kegiatan yang dilaksanakan

ID-CERT Gathering, merupakan forum pertemuan tahunan dengan konstituen dan mitra ID-CERT untuk membahas perkembangan terbaru seputar ID-CERT dan isu IT Security lainnya.

ID-CERT Gathering 2012 dilaksanakan pada 29 Pebruari 2012, dihadiri sekitar 30 orang.

3.2 Kegiatan lain

ID-CERT juga menghadiri forum pertemuan Tahunan APCERT di Bali pada 25 – 28 Maret 2012 dan dilanjutkan dengan pertemuan FIRST-TC ditempat yang sama pada 29 – 31 Maret 2012.

Kegiatan ID-CERT lainnya adalah menghadiri berbagai rapat maupun pertemuan yang diselenggarakan oleh KEMKOMINFO seperti IISF, Forum CERT Indonesia, membantu penyusunan Roadmap CERT/CC dan GovCSIRT.

Kegiatan ID-CERT yang lain adalah menjadi pembicara pada forum-forum terbatas disalah satu perbankan di Indonesia dimana ID-CERT memberikan gambaran umum serta tren IT Security dikalangan Perbankan.

ID-CERT juga diundang sebagai pembicara pada acara edukasi untuk kalangan pendidikan yang diselenggarakan di Bandung pada Januari 2012.

4 Rencana Kedepan

Hal penting yang menjadi perhatian ID-CERT untuk langkah berikutnya adalah: apa yang sebenarnya diharapkan oleh masyarakat terhadap ID-CERT.

1. ID-CERT berencana untuk terus melakukan berbagai penelitian yang diperlukan oleh komunitas internet Indonesia. Untuk itu, ID-CERT juga berencana melakukan penambahan personel di bidang penelitian ini dan bekerjasama dengan berbagai universitas terkemuka dalam membangun setiap penelitian yang dibutuhkan.
2. ID-CERT akan menerbitkan laporan penelitian secara berkala setiap bulannya, dwi bulanan, satu semester hingga laporan final setiap tahunnya.
3. ID-CERT juga menginginkan adanya dukungan konstituen terhadap edukasi publik di berbagai sektor bidang keamanan internet.

5 Dukungan Komunitas

ID-CERT berkeinginan agar semakin banyak responden yang turut serta dalam berbagai penelitian yang diadkan oleh ID-CERT, demi perbaikan internet Indonesia ke depannya. Selain itu, ID-CERT juga berkeinginan agar upaya ID-CERT dalam membangun semua ini, dapat diiringi dengan dukungan terhadap operasional ID-CERT.

5.1 Konstituen ID-CERT

Keanggotaan ID-CERT terbuka bagi seluruh komunitas internet Indonesia yang memiliki kepedulian di bidang keamanan internet, baik dari kalangan ISP maupun non-ISP seperti organisasi pemerintah (departemen, Pemda, BUMN, BUMD, dan sebagainya) maupun kalangan swasta.

5.2 Responden ID-CERT

Hingga saat ini, dari penelitian di bidang Internet Abuse 2011, ID-CERT telah mengumpulkan sebanyak 38 organisasi responden.

ID-CERT pun masih membuka diri terhadap responden baru yang ingin bergabung dalam berbagai penelitian yang diadakan ID-CERT.

5.3 Pendukung/Afiliasi ID-CERT

Para pendukung atau afiliasi ID-CERT mendefinisikannya/didefinisikan sebagai organisasi yang selama ini telah memberikan dukungan terhadap penelitian ID-CERT.

ID-CERT masih terbuka dan mengundang komunitas internet Indonesia untuk memberikan dukungannya kepada ID-CERT dalam bentuk *Sponsorship*, Donasi maupun melalui mekanisme *Membership Fees* (akan ditentukan kemudian).

*5.4 Volunteers/*Relawan ID-CERT

Sejak awal berdiri hinggi kini, ID-CERT banyak didukung oleh para *volunteers* yang bekerja tanpa pamrih memberikan kontribusi dan kepeduliannya terhadap keamanan internet Indonesia. Umumnya *volunteers* ID-CERT adalah perorangan/individu.

ID-CERT juga masih membuka kesempatan seluas-luasnya bagi individu yang ingin berkontribusi terhadap Keamanan Internet Indonesia dengan menjadi bagian dari tim peneliti ID-CERT, maupun helpdesk ID-CERT.

6 PGP Key dan Tim Kami

Alamat: Jl. Bojong Koneng Atas no 3A, Bandung 40191
Kontak Utama: **(+62)889-1400-700**
email: cert@cert.or.id
Finger Print PGP Key:15CD ADAF 7B01 B838 A795 7408 55C7 877A 4A3B E6E6

Voluntir:

1. DR. Budi Rahardjo ***(Ketua ID-CERT)***
2. Andika Triwidada ***(Wakil Ketua ID-CERT)***
   Fingerprint=5568 7C7D E898 4F33 A594 A996 DA4B C29F E22D FEE7
3. Maman Sutarman
4. Rizky Ariestiyansyah
5. Dibantu dengan sejumlah voluntir lainnya.

Staf Profesional:

1. Ahmad Alkazimy, (***Manajer ID-CERT***), ahmad@cert.or.id, M: +62-838-74-9292-15
   Finger print= 39B2 87BA 3DD6 7832 D56F 0344 FCE4 3A7C FE38 CC96
2. Rahmadian L. Arbianita, (***Incident Response Team – Helpdesk***),rahmadian@cert.or.id,
   M:(+62)811227703
   Finger print= 414A 1183 199E 8BA5 E0D1 C234 08BF 8BDE 1766 2CC7

7 Kesimpulan

Berikut ini hasil capaian ID-CERT ditahun 2012:

1. ID-CERT telah membangun *Standrard Operation Procedures* (SOP) beserta jobdesk yang jelas guna melakukan pengembangan dan penambahan personel staff, sekurang-kurangnya untuk melakukan respon helpdesk.
2. ID-CERT telah melakukan pengembangan hardware maupun software yang terkait dengan membangun mekanisme sistemik email responder dan update laman web www.cert.or.id
3. ID-CERT telah melakukan penelitian yang diperlukan oleh komunitas internet Indonesia.
4. Terhitung mulai Nopember 2012, ID-CERT secara resmi mulai mengedarkan Peringatan Keamanan / Security Advisories melalui website maupun milis.
5. ID-CERT telah menerbitkan laporan penelitian secara berkala setiap dwi bulanan, satu semester hingga laporan final setiap tahunnya diwebsite ID-CERT
6. ID-CERT ikut terlibat dalam pembentukan GovCSIRT mulai dari Roadmap hingga implementasi operasionalnya.

8 Bahan Bacaan

1. Laporan Penelitian ID-CERT: http://www.cert.or.id/incident_handling/

2. Peringatan Keamanan I – 2012 mengenai Malware Zeus: http://www.cert.or.id/indeks_berita/berita/5/

3. Peringatan Keamanan II – 2012 mengenai Malware Grumbot:
   http://www.cert.or.id/indeks_berita/berita/8/

4. Peringatan Keamanan III – 2012 mengenai saran pengamanan sistem
   http://www.cert.or.id/indeks_berita/berita/11/

5. RFC 2350 ID-CERT edisi terbaru (28 Nop 2012): http://www.cert.or.id/rfc/