

Id-SIRTII

PROGRESS REPORT 2007, 2008, 2009

INDONESIA SECURITY INCIDENT
RESPONSE TEAM
ON INTERNET INFRASTRUCTURE

Kondisi Agustus 2007 – Desember 2007

ASPECT	AGST	SEPT	OKT	NOV	DES	KETERANGAN
PIMPINAN	X	X	V	V	V	SK OKTOBER 2007
MANAJER	V	V	V	V	V	PT NCR
SDM STAFF	V	V	V	V	V	PT NCR
GEDUNG KANTOR	V	V	V	V	V	GEDUNG PT POS
FURNITURE & ATK	X	X	V	V	V	PT POS + PT NCR
AC RUANG KANTOR	X	X	V	V	V	PT POS
LISTRİK KANTOR	V	V	V	V	V	PT POS
TELEPON KANTOR	V	V	V	V	V	PT POS
INTERNET KANTOR	X	V	V	V	V	PT CNI
SERVER ROOM	X	X	X	X	X	TIDAK ADA
AC SERVER ROOM	X	X	X	X	X	TIDAK ADA
MONITORING ROOM	X	X	X	X	X	TIDAK ADA
DATA CENTER	V	V	V	V	V	PT POS
CO-LOCATION	V	V	V	V	V	APJII (IIX)
INTERNET BACKUP	X	X	X	X	X	TIDAK ADA
FIBER OPTIC LINK	X	V	V	V	V	PT CNI
AKTIVASI SENSOR *)	X	X	V	V	V	TELKOM & OIXP
BIAYA OPERASIONAL	V	V	V	V	V	PT NCR

*) XL, CBN, INDONET, INDOSAT, IM2, NAPINFO, IIX (TELKOM & OIXP MENOLAK – ALASAN LEGAL)

Kondisi Januari 2008 – Mei 2008

ASPECT	JAN	FEB	MAR	APR	MEI	KETERANGAN
PIMPINAN	V	V	V	V	V	SOSIALISASI *)
MANAJER	X	X	X	X	X	BELUM ADA PT
SDM STAFF	X	X	X	X	X	BELUM ADA PT
GEDUNG KANTOR	V	V	V	V	V	BELUM ADA GEDUNG
FURNITURE & ATK	X	X	V	V	V	BELUM ADA GEDUNG
AC RUANG KANTOR	X	X	V	V	V	BELUM ADA GEDUNG
LISTRİK KANTOR	V	V	V	V	V	BELUM ADA GEDUNG
TELEPON KANTOR	V	V	V	V	V	BELUM ADA GEDUNG
INTERNET KANTOR	X	V	V	V	V	BELUM ADA GEDUNG
SERVER ROOM	X	X	X	X	X	TIDAK ADA
AC SERVER ROOM	X	X	X	X	X	TIDAK ADA
MONITORING ROOM	X	X	X	X	X	TIDAK ADA
DATA CENTER	X	X	X	V	V	PINDAH KE LT. 24 POSTEL
CO-LOCATION	V	V	V	V	V	APJII (IIX)
INTERNET BACKUP	X	X	X	X	X	BELUM ADA PT
FIBER OPTIC LINK	X	X	X	X	X	BELUM ADA PT
AKTIVASI SENSOR **)	V	V	V	V	V	INDOSAT & OIXP
BIAYA OPERASIONAL	X	X	X	X	X	BELUM ADA PT

*) BIAYA SENDIRI (10 PEMDA, PULUHAN INSTANSI, PERGURUAN TINGGI, KUNJUNGAN 5 NEGARA MENGADAKAN WORKSHOP DAN SEMINAR, ASISTENSI (BANK, BUMN, ISP, SWASTA DLL.)

**) XL, CBN, INDONET, NAPINFO, TELKOM, IIX (INDOSAT, IM2 & OIXP MENOLAK – ALASAN LEGAL)

Kondisi Juni 2008 – Desember 2008

ASPECT	JUNI	JULI	AGST	SEP	OKT	NOV	DES	KETERANGAN
PIMPINAN	V	V	V	V	V	V	V	FOKUS MONITORING
MANAJER	V	V	V	V	V	V	V	KONTRAK PERORANGAN
SDM STAFF	V	V	V	V	V	V	V	PT MULTISOEK
GEDUNG KANTOR	V	V	V	V	V	V	V	MENARA RAVINDO
FURNITURE & ATK	V	V	V	V	V	V	V	POSTEL *)
AC RUANG KANTOR	V	V	V	V	V	V	V	MENARA RAVINDO **)
LISTRİK KANTOR	V	V	V	V	V	V	V	MENARA RAVINDO
TELEPON KANTOR	V	V	V	V	V	V	V	MENARA RAVINDO
INTERNET KANTOR	V	V	V	V	V	V	V	PT CNI
SERVER ROOM	V	V	V	V	V	V	V	TIDAK STANDAR
AC SERVER ROOM	X	X	X	X	X	X	X	TIDAK ADA
MONITORING ROOM	V	V	V	V	V	V	V	TIDAK STANDAR ***)
DATA CENTER	V	V	V	V	V	V	V	PINDAH KE LT. 24 POSTEL
CO-LOCATION	V	V	V	V	V	V	V	APJII (IIX)
INTERNET BACKUP	V	V	V	V	V	V	V	SPEEDY TELKOM
FIBER OPTIC LINK	V	V	V	V	V	V	V	PT CNI
AKTIVASI SENSOR	V	V	V	V	V	V	V	#) KECUALI INDOSAT & OIXP
BIAYA OPERASIONAL	V	V	V	V	V	V	V	PT MULTISOEK, UTANG 45 JT

*) KEKURANGAN KURSI (PINJAM YAYASAN KUWERA DAN PT USADI SERTA MILIK PRIBADI) KARENA TIDAK ADA ANGGARAN

DAN JUMLAH PC TERBATAS, KEKURANGAN UNTUK MONITORING, KEKURANGAN NOTEBOOK UNTUK MOBILITAS TIM TEKNIS

**) TIDAK 24 JAM, HANYA PADA JAM KANTOR 08.00 – 18.00 DAN SERING MENGALAMI GANGGUAN (MATI, TIDAK DINGIN DLSB.)

***) BENTUK RUANGAN TIDAK SESUAI STANDAR, TIDAK ADA PENGAMANAN YANG MEMADAI (KAMERA SURVEILLANCE DLSB.)

#) XL, CBN, INDONET, NAPINFO, TELKOM, BIZNET, CENTRIN, IIX (INDOSAT, IM2 & OIXP MENOLAK – ALASAN LEGAL)

Kondisi Januari 2009 – Maret 2009

ASPECT	JAN	FEB	MAR	KETERANGAN
PIMPINAN	V	V	V	FOKUS MONITORING DAN LOG
MANAJER	X	V	V	KONTRAK PERORANGAN MULAI FEBRUARI, JANUARI TIDAK DIBAYAR
SDM STAFF	V	V	V	PT BUDI, KONTRAK MULAI FEBRUARI, JANUARI TIDAK DIBAYAR
GEDUNG KANTOR	V	V	V	MENARA RAVINDO
FURNITURE & ATK	V	V	V	POSTEL, PINJAM PAKAI YAYASAN KUWERA DAN PT USADI
AC RUANG KANTOR	V	V	V	MENARA RAVINDO, TIDAK 24 JAM, 08.00 – 18.00
LISTRİK KANTOR	V	V	V	MENARA RAVINDO, PERLU TAMBAH DAYA LAB. + TRAINING CENTER
TELEPON KANTOR	V	V	V	MENARA RAVINDO
INTERNET KANTOR	V	V	V	PT CNI
SERVER ROOM	V	V	V	TIDAK STANDAR, PERLU PENINGKATAN DAN TAMBAHAN RACK
AC SERVER ROOM	X	X	X	TIDAK ADA, PERLU PENAMBAHAN AC 24 JAM
MONITORING ROOM	V	V	V	TIDAK STANDAR, PERLU RENOVASI + CAMERA SURVEILLANCE
DATA CENTER	V	V	V	LT. 24 POSTEL
CO-LOCATION	V	V	V	APJII (IIX)
INTERNET BACKUP	V	V	V	SPEEDY TELKOM
FIBER OPTIC LINK	V	V	V	PT CNI
AKTIVASI SENSOR	V	V	V	*) KECUALI INDOSAT & OIXP
BIAYA OPERASIONAL	X	X	X	POSTEL, BELUM ADA PENCAIRAN DAN REIMBURST

*) XL, CBN, INDONET, NAPINFO, TELKOM, BIZNET, CENTRIN, IIX (INDOSAT, IM2 & OIXP MENOLAK – ALASAN LEGAL)

Kondisi Monitoring 22 Februari 2009 – 13 Maret 2009

ASPECT	EXPECTATION	ALLOCATION	IMPLEMENTATION
SENSOR	30 NAP + 2 IX	9 NAP + 2 IX	9 NAP + 2 IX
BACKUP	REDUNDANT	2 SENSOR + 1 MC	NO BACKUP
CAPACITY	FIT TO TRAFFIC GROWTH	4 GBIT/S + 10 GBIT/S IX	10 GBIT/S + 15 GBIT/S IX (EXPONENTIAL)
OPERATION	24/7, 3 SHIFT	OFFICE HOUR ONLY, 1 SHIFT	24/7, UNPAID OVERTIME
LICENSE	UPGRADE YEARLY	NO ALLOCATION	PROBLEM, NO SUPPORT
SURVEILLANCE	LT. 24 + RAVINDO	LT. 24 + RAVINDO	LT. 24 + RAVINDO
DATA CENTER	FIT TO SPACE NEEDED	NO ALLOCATION	OVERLOAD, OVERHEAT
SECURITY	MANAGED SECURITY	NO ALLOCATION	NOT COMPLY WITH CERT/CSIRT STANDARD
KM/PERDIR	PEMANFAATAN DATA	NO ALLOCATION	BELUM ADA DRAFT

1. MONITORING DIHENTIKAN: CENTRAL DATABASE MANAGEMENT CONSOLE (MC3000) SOURCEFIRE CORRUPT, NO SPARE UNIT
- 2.2 UNIT SOURCEFIRE BARU BELUM BISA DIAKTIFKAN DAN DIINTEGRASIKAN KARENA VERSI FIRMWARE TIDAK SAMA
3. BELUM BISA UPGRADE KARENA LISENSI DAN SUPPORT SUDAH EXPIRED (PER 26 DESEMBER 2008)
- 4.2 IBM SERVER + 1 APC SURTX6000 RACK UPS MATI AKIBAT OVERHEATING (KEKURANGAN SPACE RACK), NO SPARE UNIT

Solusi Yang Sudah Diusulkan ID-SIRTII

- MEMINTA DUKUNGAN ONLINE TIDAK RESMI SOURCEFIRE PUSAT DI AMERIKA UNTUK MEMPERBAIKI MANAGEMENT CONSOLE
- MEMINTA PENDAMPINGAN (VISITE) TEKNISI SOURCEFIRE DARI MALAYSIA UNTUK UPGRADE FIRMWARE 11 UNIT SENSOR
- MENGAJUKAN APBN-P UNTUK LICENSE RENEWAL 9 UNIT SENSOR + 1 MANAGEMENT CONSOLE BERLAKU HINGGA DESEMBER
- MENGAJUKAN APBN-P UNTUK PENGADAAN 1 SPARE UNIT (BACKUP) PERANGKAT MANAGEMENT CONSOLE (MC3000)
- MENGANGGARKAN LICENSE RENEWAL 11 UNIT SENSOR + 2 MANAGEMENT CONSOLE SETIAP TAHUN SEJAK 2010
- MENGAJUKAN APBN-P PENAMBAHAN UNIT RACK + BLOWER + SEWA SPACE DI DATACENTER APJII (IIX) LT.1 GEDUNG CYBER
- MENGAJUKAN APBN-P PENAMBAHAN AC RUANG SERVER DI RAVINDO + BIAYA SEWA SPACE ROOF TOP GEDUNG BULANAN

Perkembangan Sejak 13 Maret 2009

- BERKAT KOORDINASI DAN DUKUNGAN TIDAK RESMI DARI SOURFIRE PUSAT, KERUSAKAN BERHASIL DIPULIHKAN
- BERKAT BANTUAN TEKNISI SOURCEFIRE DARI MALAYSIA (BERKUNJUNG MELAKUKAN PENDAMPINGAN 3 HARI SEJAK SENIN 16 MARET 2009, PERANGKAT BERHASIL DIUPGRADE)
- TAGIHAN KEGIATAN VISITE TEKNISI MALAYSIA SUDAH DIAJUKAN KE POSTEL, SEDANG MENUNGGU PERSETUJUAN
- RABU 18 MARET 2009 ID-SIRTII MENGAJUKAN USULAN ANGGARAN APBN P-2008 DAN RENCANA ANGGARAN 2010
- ANGGARAN APBN-P 2008 YANG DIAJUKAN TERMASUK UNTUK PERANGKAT BACKUP DAN RENEWAL LISENSI

Pengelolaan Log File Tahun 2007 – 2009

ASPECT	EXPECTATION	ALLOCATION	IMPLEMENTATION
PERDIR TATA CARA LOG	SESUAI KEBUTUHAN	POSTEL	227/2007
PERDIR PENEMPATAN ALAT	SESUAI KEBUTUHAN	POSTEL	225/2008
PERDIR PENYELARASAN WAKTU	SESUAI KEBUTUHAN	POSTEL	DRAFT (APRIL 2008)
PERDIR PENCATATAN IDENTITAS	SESUAI KEBUTUHAN	POSTEL	DRAFT (APRIL 2008)
PERDIR TIM RESPON INSIDEN	SESUAI KEBUTUHAN	POSTEL	DRAFT (APRIL 2008)
DATA CENTER DAN STORAGE	SESUAI PERENCANAAN	POSTEL, ID-SIRTII	READY, (?) CAPACITY *)
SISTEM PENERIMAAN	SESUAI PERENCANAAN	POSTEL, ID-SIRTII	READY, UJI COBA *)
UJI COBA NAP / ISP	7 NAP DI JAKARTA	TIDAK ADA	3 NAP JKT, 2 ISP DAERAH *)
SOSIALISASI KONSTITUEN	SEMAKSIMAL MUNGKIN	1 SEMINAR NASIONAL	1 SEMINAR, PULUHAN VISITE
PROOF OF CONCEPT	MELIBATKAN VENDOR	TIDAK ADA	HANYA DENGAN ISP
ASISTENSI TIM AHLI	SEMAKSIMAL MUNGKIN	5 RAPAT, 2 KONSINYERING	TIDAK ADA

Permasalahan Log File

- BESARAN DATA, UJI COBA XL UNTUK 2 GBIT/S TRAFFIC MENGHASILKAN 30 GBYTES DATA DALAM 30 MENIT
- MEMPENGARUHI KINERJA PERANGKAT DAN PERFORMA JARINGAN (MENINGKATNYA UTILISASI ALAT & LATENCY)
- DIPERLUKAN INVESTASI PERALATAN BARU DAN ATAU UPGRADE SERTA ALOKASI SALURAN UNTUK PENGIRIMAN
- SISTEM PENERIMAAN DAN PENYIMPANAN ID-SIRTII BELUM TERUJI (PROVEN) UNTUK MELAYANI PENGIRIMAN RIIL
- RESISTENSI ISP KARENA BESARNYA KONSEKUENSI BIAYA DAN TIDAK ADANYA INSENTIF SERTA ISU REGULASI
- PERLU KETEGASAN REGULATOR TERHADAP KOMITMEN OPERATOR & PENGUATAN DASAR HUKUM LOG FILE

Rekomendasi ID-SIRTII

- MERUMUSKAN KEMBALI REGULASI DAN DASAR HUKUM DAN KONSEP IMPLEMENTASI TEKNIS LOG BERSAMA TIM AHLI
- MELAKUKAN SOSIALISASI KEPADA ISP, DILAKSANAKAN OLEH TIM AHLI DAN POSTEL MELIBATKAN PENEGAK HUKUM (TIDAK DIBEBANKAN KEPADA ID-SIRTII, KARENA KEWENANGANNYA HANYA PELAKSANA)
- MENERAPKAN KEWAJIBAN LOG FILE INI SEJAK DARI PENGAJUAN PROPOSAL BISNIS CALON ISP DAN MENJADI SALAH SATU CHECKLIST UJI LAIK OPERASI (ULO) UNTUK ISP DAN DIUMUMKAN SECARA TERBUKA
- MELAKUKAN SOSIALISASI KEPADA PENEGAK HUKUM UNTUK MEMANFAATKAN LOG FILE (POLISI, JAKSA, HAKIM, KPK) SEBAGAI ALAT BUKTI YANG DIMINTAKAN KE ISP

Sosialisasi Tahun 2007 – 2009

ASPECT	EXPECTATION	ALLOCATION	IMPLEMENTATION
KUNJUNGAN DINAS	20 KOTA/KABUPATEN /INSTANSI	5 KOTA/KABUPATEN	40 KOTA, 20 INSTANSI
SEMINAR BESAR (JAKARTA)	3 SEMINAR NASIONAL, 1 INTL.	1 SEMINAR NASIONAL	5 NASIONAL, 1 INTL. (MY)
WORKSHOP DI DAERAH	5 NON IBUKOTA PROVINSI	TIDAK ADA	5 INSTANSI DI DAERAH
PUBLIKASI MEDIA	SEBANYAK MUNGKIN	TIDAK ADA	2 LIPUTAN TV, 30 BERITA, 112 RIBU
PENERBITAN MATERI	SEBANYAK MUNGKIN	TIDAK ADA	50 RIBU POSTER, 2 PANDUAN
INTERNET SEHAT & AMAN	SEBANYAK MUNGKIN	TIDAK ADA	ROAD SHOW, 1 SET PANDUAN + TOOLS

Asistensi Teknis Tahun 2007 – 2009

ASPECT	EXPECTATION	ALLOCATION	IMPLEMENTATION
DITJEN PAJAK	SEBANYAK MUNGKIN	TIDAK ADA	2 KASUS, TRAINING
KEPOLISIAN (PENEGAK HUKUM)	SEBANYAK MUNGKIN	TIDAK ADA	BELASAN KASUS, TRAINING
INSTANSI INTELEJEN	SEBANYAK MUNGKIN	TIDAK ADA	DESAIN TEKNIS, WORKHSOP
BI, BUMN, BANK, CRITICAL INF.	SEBANYAK MUNGKIN	TIDAK ADA	BELASAN KASUS, DESAIN TEKNIS, TRAINING
KOMISI PEMILIHAN UMUM	SEOPTIMAL MUNGKIN	5 RAPAT	DIBATALKAN
PEMDA, UNIVERSITAS, ORMAS	SEBANYAK MUNGKIN	TIDAK ADA	BELASAN DESAIN TEKNIS, WORKHSOP

Layanan Informasi Publik Tahun 2007 – 2009

ASPECT	EXPECTATION	ALLOCATION	IMPLEMENTATION
HELP DESK CALL CENTER	SEBANYAK MUNGKIN	TIDAK ADA	2007, SISTEM SIAP - KETERBATASAN SDM 2008, SISTEM SIAP – KETERBATASAN SDM 2009, REKONFIGURASI SISTEM & SDM
KNOWLEDGE REPOSITORTY	SEBANYAK MUNGKIN	TIDAK ADA	2007, SISTEM SIAP - KETERBATASAN SDM 2008, SISTEM SIAP – KETERBATASAN SDM 2009, REKONFIGURASI SISTEM & SDM
WEB SITE RESMI	SEBANYAK MUNGKIN	TIDAK ADA	2007, SISTEM SIAP - KETERBATASAN SDM 2008, SISTEM SIAP – KETERBATASAN SDM 2009, REKONFIGURASI SISTEM & SDM
VULNERABILITY REPOSITORY	SEBANYAK MUNGKIN	TIDAK ADA	2007, SISTEM SIAP - KETERBATASAN SDM 2008, SISTEM SIAP – KETERBATASAN SDM 2009, REKONFIGURASI SISTEM & SDM

Kerjasama Antar Lembaga Tahun 2007 – 2009

ASPECT	EXPECTATION	ALLOCATION	IMPLEMENTATION
MOU INTERNATIONAL	2 NEGARA	TIDAK ADA	2 NEGARA
MOU KEMITRAAN	SEBANYAK MUNGKIN	TIDAK ADA	3 MITRA, 2 UNIV., 1 VENDOR
KOORDINASI INSIDEN	SEOPTIMAL MUNGKIN	TIDAK ADA	PULUHAN KASUS
KERJASAMA TEKNIS	SEBANYAK MUNGKIN	TIDAK ADA	3 COMMUNITY PROJECT
KUNJUNGAN INTERNASIONAL	16 NEGARA ANGGOTA APCERT	TIDAK ADA	7 NEGARA

Riset dan Pengembangan Tahun 2007 – 2009

ASPECT	EXPECTATION	ALLOCATION	IMPLEMENTATION
MALWARE ANALYSIS	SEOPTIMAL MUNGKIN, 2009	PENGADAAN LAB. SAJA, 2009	2008, SGU + PERBANAS + KKI
DIGITAL FORENSIC	SEOPTIMAL MUNGKIN, 2009	PENGADAAN LAB. SAJA, 2009	2008, SGU + PERBANAS + KKI
ANTI SPAM TECHNOLOGY	SEOPTIMAL MUNGKIN, 2009	PENGADAAN LAB. SAJA, 2009	2009, SGU + VENDOR + KKI
DATA MINING TECHNOLOGY	SEOPTIMAL MUNGKIN, 2009	PENGADAAN LAB. SAJA, 2009	2008, SGU + PERBANAS + KKI
LABORATORIUM SIMULASI	SEOPTIMAL MUNGKIN, 2009	PENGADAAN LAB. SAJA, 2009	AKAN PENGADAAN JUNI 2009
PUSAT PELATIHAN	SEOPTIMAL MUNGKIN, 2009	PENGADAAN LAB. SAJA, 2009	2008, YAYASAN KUWERA + KKI
HONEYNET PROJECT	SEOPTIMAL MUNGKIN, 2008	PENGADAAN LAB. SAJA, 2009	2008, SGU + PERBANAS + KKI
NAWALA PROJECT *)	SEOPTIMAL MUNGKIN, 2008	TIDAK ADA	2008, AWARI + KKI

SELURUH KEGIATAN DI ATAS TIDAK ADA ALOKASI ANGGARAN RISET DAN OPERASIONALNYA.

*) CONTENT FILTERING, ANTI PHISING SITE, ANTI MALWARE, ANTI SPAM, NATIONAL DNS RESOLVER, NTP SERVER (4 JUTA HITS)

Permasalahan SDM

- MENURUT KELLY SERVICES, GAJI SDM TEKNIS LEMBAGA SEPERTI ID-SIRTII MINIMUM 7 JUTA, REALISASI TAHUN 2007 = 4 JUTA MAKSIMUM, 2008 = 4 JUTA MAKSIMUM (RATA-RATA 2,5 JUTA), 2009 = 4 JUTA MAKSIMUM
- OUTSOURCING MENGURANGI PENYERAPAN ANGGARAN HINGGA 40% (PAJAK, KEUNTUNGAN PT, ADMINISTRASI)
- MENURUT KELLY SERVICES, GAJI MANAJER MINIMUM 12 JUTA, REALISASI TAHUN 2007, 2008, 2009 < 10 JUTA
- KONTRAK TAHUNAN MENGAKIBATKAN RESIKO TERHADAP INTEGRITAS SDM BERKAITAN DENGAN KERAHASIAAN DATA
- BENEFIT YANG DITAWARKAN TIDAK MENARIK, TERBUKTI MINAT PESERTA LELANG SDM & OUTSOURCING RENDAH

Realisasi SDM

YEAR	EXPECT EMPLOY	REAL EMPLOY	EXPECT SALARY	REAL SALARY	QUALITY
2007	27 STAFF	15 STAFF	7 MIL MIN	4 MIL MAX 3 MIL AV	MEDIUM
	5 MNGR	5 MNGR	12 MIL MIN	< 10 MIL	HIGH
2008	27	18	7 MIL MIN	4 MIL MAX 2,5 MIL AV	LOW SKILL
	5 MNGR	5 MNGR	12 MIL MIN	< 10 MIL	HIGH
2009	29 *)	23	7 MIL MIN	4 MIL MAX 3 MIL AV	MED HIGH
	5 MNGR	5 MNGR	12 MIL MIN	< 10 MIL	HIGH

***) TERMASUK 2 ORANG PENGEMUDI – TIDAK ADA MOBIL DINAS**