

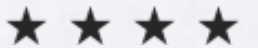


Id-SIRTII



TRANSISI PENGEMBANGAN

“Pusat Pelaporan dan Koordinasi Insiden, Layanan Publik”



REGULASI

ROAD MAP

- * Peraturan Menteri Nomor 26/PER/M.KOMINFO/5/2007
- * Peraturan Menteri Nomor 16/PER/M.KOMINFO/10/2010
- * Beberapa Peraturan Dirjen Postel sebagai pendukung operasional
- * Rencana akan disempurnakan dalam PERMEN baru pada 2011, menyesuaikan dengan struktur baru Kementerian
- * Rencana akan diamankan dalam pasal RUU konvergensi dan akan diturunkan dalam bentuk PP atau Perpres
- * Rancangan Perdir/Permen Penyelarasan Waktu Server *)

KETERKAITAN LAIN

- * Kepentingan terhadap isu Cyber Security, menarik minat sektor lain dan karenanya ID-SIRTII memberikan masukan kepada:
- * Sektor Perbankan, terutama Bank Indonesia akan menerbitkan peraturan yang lebih memperhatikan masalah Cyber Security
- * Sektor Hankam, masalah Cyber Security akan diusahakan untuk dimasukkan dalam 4 paket RUU Hankam yaitu RUU Keamanan Nasional, RUU Rahasia Negara, RUU Intelejen, RUU Komponen Cadangan (Cyber Army)
- * Sektor Telekomunikasi, BRTI akan mengusulkan regulasi standar keamanan telekomunikasi

HAMBATAN

- * Dasar hukum yang kurang kuat mengakibatkan lemahnya upaya untuk meningkatkan kepatuhan industri terhadap fungsi, tugas ID-SIRTII antara lain dalam penempatan perangkat sensor dan pengumpulan log (selain karena masalah teknis)
- * Kewenangan yang terbatas dan berada jauh di bawah (setingkat Eselon II) mengakibatkan kurangnya antusiasme politis dari para pejabat di lingkungan instansi lain (strategis)
- * Kelembagaan dan fungsi yang belum permanen mengakibatkan sulitnya membangun relasi dan kerjasama dengan pihak lain yang bersifat mengikat dan jangka panjang
- * Tidak ada dasar kuat untuk menyelenggarakan layanan publik

LAYANAN DASAR

SISTEM PEMANTAUAN

- * Meningkatkan kapasitas dan ruang lingkup pemantauan di 30 NAP
- * Menyusun prioritas pemantauan: Infrastruktur Kritis, NAP, ISP, IX
- * Membuka akses pemantauan kepada NAP, ISP, IX yang dipantau
- * Membuka layanan pengaduan untuk publik (tidak hanya NAP, ISP)
- * Meningkatkan kapasitas analisa dan menyajikan hasil pada publik (security alert, security advisory, koordinasi nasional/CC)
- * Meningkatkan layanan Early Warning, asistensi mitigasi insiden

PENGUMPULAN LOG

- * Perlu evaluasi dan pembahasan ulang skenario teknis pelaksanaan dan efektivitasnya serta manfaatnya bersama TIM AHLI ID-SIRTII
- * Peningkatan kapasitas dan pelaksanaan pengumpulan log file
- * Informasi log file belum cukup membantu proses penegakan hukum sebagaimana semula diharapkan. Untuk penyidikan para penegak hukum lebih membutuhkan bantuan keterlibatan dari para expert analis secara langsung dan layanan digital forensic
- * Untuk kepentingan mitigasi insiden, log file sebaiknya tetap ada setiap NAP, ISP, IX hingga ke tingkat jaringan distribusi

FASILITAS PELATIHAN

- * Menyelenggarakan training untuk 1000+ orang sesuai program anggaran 2011, outsourcing dan kerjasama dengan pihak ketiga
- * Training reguler untuk umum: guru, mahasiswa, jurnalis, instansi dengan materi pokok Cyber-6 serta TOT
- * Training khusus sesuai permintaan: instansi sipil/militer, BUMN
- * Training in house untuk industri sesuai permintaan: NAP/ISP
- * Training lainnya/spesifik: materi Open Source dan Security, IT Forensic, Certified EC-Council, Certified CSSIP etc.
- * Produksi video tutorial kesadaran informasi dan self training

KESADARAN INFORMASI

- * Portal ID-SIRTII, terhubung ke social media dan situs global
- * ID-KIDS, portal pendampingan anak untuk mengakses Internet
- * Material kesadaran: video animasi, poster, leaflet, booklet, buletin tutorial internet self defense, training duta keamanan informasi
- * Road show 5 kota bersama POSTEL, ++ bersama komunitas
- * Kerjasama dengan ICT Watch, AWARI, KKI, APTIKOM

KOORDINASI

- * Telah diterima sebagai anggota APCERT (2009) dan Full Member (2010), FIRST (on process, akan diumumkan next AGM 2011) dan anggota pendiri OIC-CERT
- * Mengikuti aktifitas koordinasi internasional di APCERT, FIRST, drill test, pertukaran staf dengan MyCERT, workshop/collaqioum
- * Bersama POSTEL berpartisipasi di forum ITU, APT, APEC dll.
- * Meningkatkan kegiatan Forum Tim Respon Insiden Nasional

RISET PENGEMBANGAN

- * More Tsubame Sensors (3 more units)
- * Malware Analysis & Data Mining Program
- * Nation Wide Honey Net Program
- * Continue Anti SPAM & Secure DNS Program
- * Enhancing Threat Information Coordination
- * Improving Security Technical Training

RISET PENGEMBANGAN

- * Promote National Information Security Policies
- * National Internet Child Protection Program
- * Peningkatan Digital Forensics Laboratory
- * Open Source and Secure Tools Repository
- * National Secure Data Center and Internet Exchange Design
- * Secure Content Delivery Network

ID-SIRTII

- * Ravindo Tower 17th Floor
- * Kebon Sirih Raya, Kav. 75
- * Central Jakarta, 10340
- * Phone +62 21 3192 5551 ; Fax +62 21 3193 5556
- * info@idsirtii.or.id ; www.idsirtii.or.id
- * We look forward for future cooperation with you all. Thank you.