diskominfo jabar

JABARPROV CSIRT

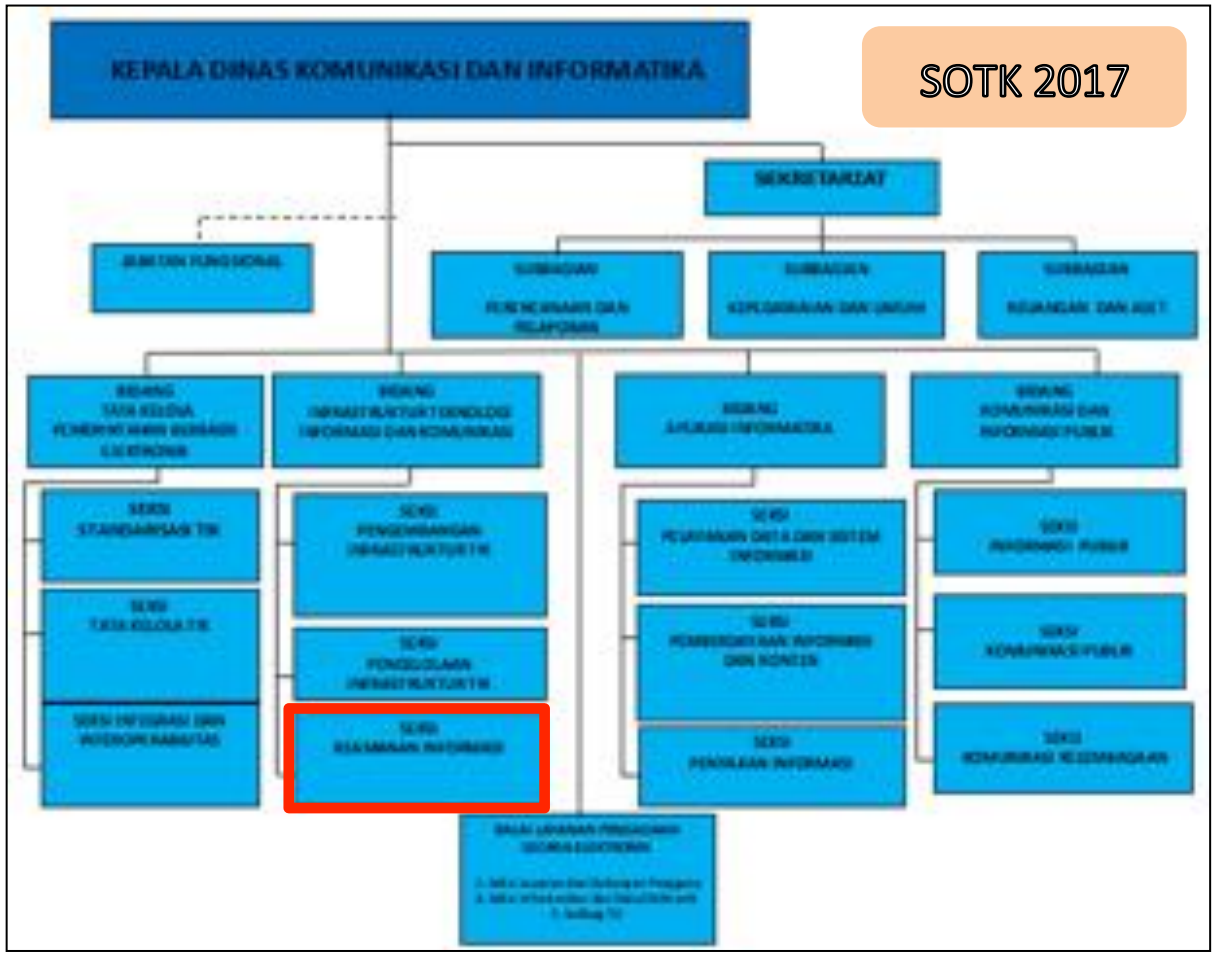
Computer Security Incident Response Team

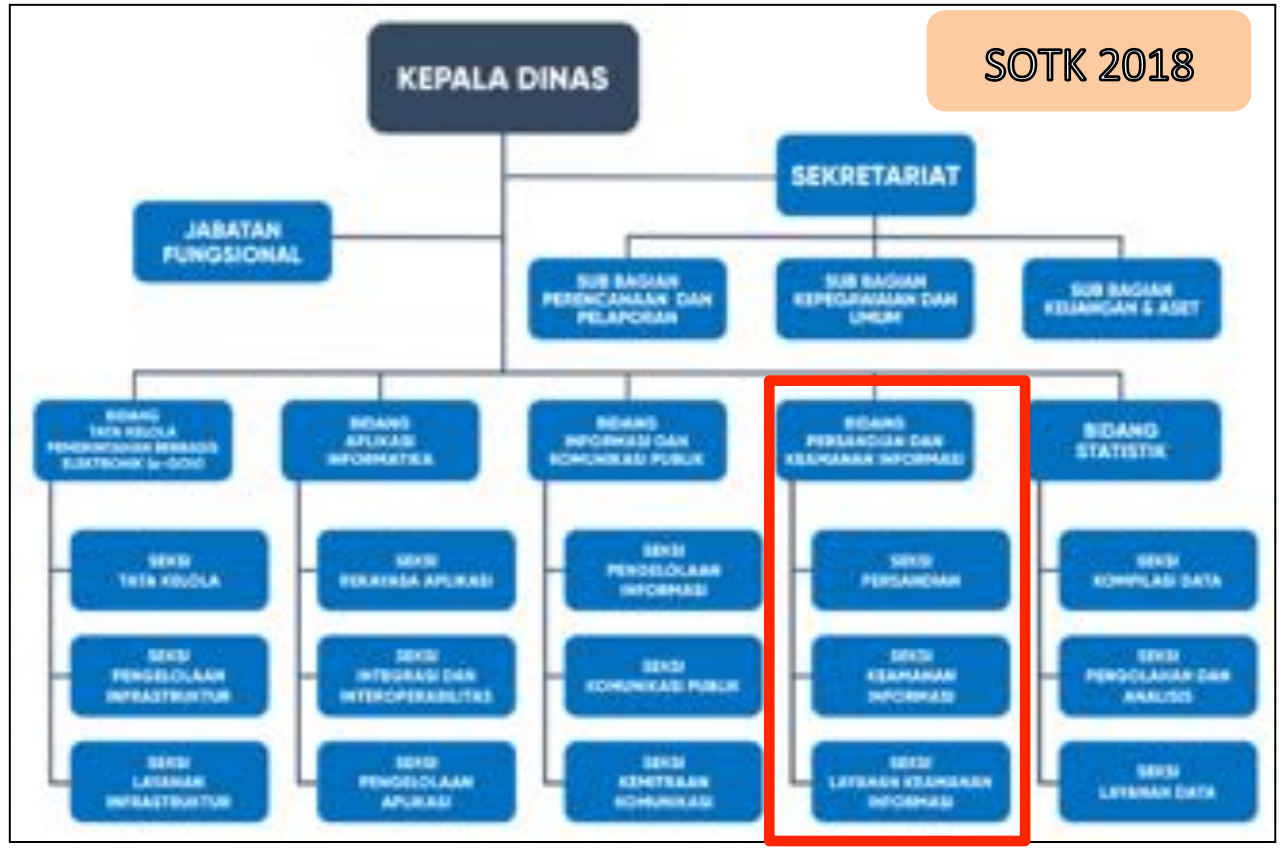
oleh:
Dr. Hening Widiatmoko, MA

Pembagian Kewenangan Urusan Persandian dan Keamanan Informasi Berdasarkan UU No 23 Tahun 2014

NO	SUB URUSAN	PEMERINTAH PUSAT	DAERAH PROVINSI	DAERAH KABUPATEN/KOTA
1	2	3	4	5
1.	Persandian untuk Pengamanan Informasi	a. Penyelenggaraan persandian untuk pengamanan informasi Pemerintah Pusat. b. Penetapan pola hubungan komunikasi sandi antar-kementerian/lembaga, antara Pemerintah Pusat dengan Daerah provinsi dan Daerah kabupaten/kota. c. Pengelolaan kunci sandi.	a. Penyelenggaraan persandian untuk pengamanan informasi Pemerintah Daerah provinsi. b. Penetapan pola hubungan komunikasi sandi antar-Perangkat Daerah provinsi.	a. Penyelenggaraan persandian untuk pengamanan informasi Pemerintah Daerah kabupaten/kota. b. Penetapan pola hubungan komunikasi sandi antar-Perangkat Daerah kabupaten/kota.

Struktur Organisasi Dinas Kominfo Jabar



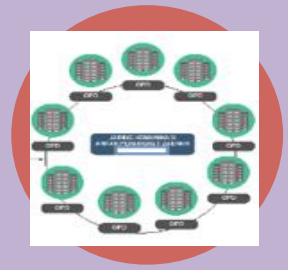


Pada SOTK Tahun 2018, Seksi Keamanan Informasi ditingkatkan levelnya menjadi Bidang Persandian dan Keamanan Informasi yang terdiri dari 3 (Tiga) Seksi, yaitu Seksi Persandian, Seksi Keamanan Informasi, dan Seksi Layanan Keamanan Informasi

Layanan Bidang Persandian dan Keamanan Informasi

Pengelolaan Sertifikat Elektronik

Pam Info Publik dan Berklasifikasi: Tanda Tangan Digital, Mail Protection, Document Protection, SSL Server, dan SSL Client



Pengelolaan Jaring Komunikasi Sandi (JKS)

Pam Info Berklasifikasi via JKS Internal: VIP Provinsi, Antar Perangkat Daerah, Intra Perangkat Daerah, dan JKS Eksternal

Sterilisasi Kontra Penginderaan

Pam Info pada Aset/Fasilita Penting: Deteksi Upaya Penyadapan Pihak Tidak Berwenang

Jamming

Pam Info dan Pam FIsik Kegiatan Penting

IT Security Assessment

Penilaian Keamanan Sistem Informasi : Vulnerable Assessment dan Penetration Testing

Pengelolaan Security Operation Center

Pam Info: pengawasan, perlindungan, dan penanggulangan insiden keamanan informasi, kolaborasi dg NOC

Digital Forensic Kepentingan Internal

Investigasi, analisa, recovery, dan management data dari media digital untuk kepentingan internal

Audit dan Sertifikasi Keamanan Informasi

Sertifikasi - Opini dan Keyakinan Yang Memadai tentang Keamanan Informasi Untuk Eskternal/Publik

Opini dan Keyakinan tentang Keamanan Informasi/ Persandian untuk Internal

DASAR HUKUM

Peraturan Kepala Lembaga Sandi Negara Nomor 7 Tahun 2017 tentang Pedoman Penyelenggaraan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintahan Daerah Provinsi dan Kabupaten/Kota.

Bidang Persandian dan Keamanan Informasi Memiliki Tugas untuk Mengelola Insiden Keamanan Informasi di dalam wadah layanan SOC (Security Operation Center)

INSIDEN KEAMANAN INFORMASI & CSIRT

Insiden Keamanan Informasi adalah setiap kejadian yang dapat menyebabkan gangguan pada sistem komputer, seperti serangan virus, akses illegal, kebocoran informasi, serangan DDOS, dan lain sebagainya.

CSIRT (Computer Security Incident Response Team) adalah sebuah Tim yang dibentuk untuk merespon insiden keamanan informasi yang terjadi pada konstituennya. Tujuan utama dari respon / tanggapan terhadap insiden adalah untuk menghentikan insiden agar tidak menyebar serta agar sistem yang terinfeksi dapat beroperasi secara normal

JabarProv-CSIRT

LATAR BELAKANG

Banyaknya insiden (*spam*, *malware*, *deface*, *phishing*) terhadap aset TIK instansi pemerintah

TUJUAN

Mengamankan dan mengurangi insiden keamanan informasi di jajaran Perangkat Daerah Pemprov Jawa Barat

Launching JabarProv-CSIRT 3 Desember 2015 di Gedung Sate

Pemerintah Provinsi Jawa Barat melalui Dinas Komunikasi dan Informatika Provinsi Jawa Barat melaunching pembentukan "Jabar Provincial Goverment Computer Security Incedent Response Team" (JabarProv-CSIRT), Tanggal 3 Desember 2015, bertempat di Aula Barat Gedung Sate Bandung, di hadapan para pengelola teknologi informasi dan komunikasi Kab/Kota Jawa Barat dan beberapa OPD Lingkup Prov. Jabar.

Pembentukan JabarProv-CSIRT merupakan tindak lanjut dari inisiasi Kementerian Komunikasi dan Informatika RI untuk membentuk CSIRT di Pemerintah Daerah.


PEMERINTAH PROVINSI JAWA BARAT
DINAS KOMUNIKASI DAN INFORMATIKA

KEPUTUSAN
KEPALA DINAS KOMUNIKASI DAN INFORMATIKA
PROVINSI JAWA BARAT

TENTANG

PEMBENTUKAN TIM JAWA BARAT PROVINSI
COMPUTER SECURITY INCIDENT RESPONSE TEAM (JabarProv-CSIRT)

Email Aduan JabarProv-CSIRT :
abuse@csirt.jabarprov.go.id

JabarProv-CSIRT Tahun 2018

PEMERINTAH PROVINSI JAWA BARAT
DINAS KOMUNIKASI DAN INFORMATIKA
Jalan Tamansari No. 55 Telepon (022) 2502898 Fax (022) 2511505
http://diskominfo.jabarprov.go.id
email : diskominfo@jabarprov.go.id
BANDUNG 40132

KEPUTUSAN
KEPALA DINAS KOMUNIKASI DAN INFORMATIKA
PROVINSI JAWA BARAT

NOMOR: 046 / Kep.1246 / Diskominfo
TENTANG
COMPUTER SECURITY INCIDENT RESPONSE TEAM
PROVINSI JAWA BARAT (JabarProv-CSIRT)

KEPALA DINAS KOMUNIKASI DAN INFORMATIKA
PROVINSI JAWA BARAT,

Menimbang

a. bahwa untuk meningkatkan kualitas pelayanan publik Pemerintah Provinsi Jawa Barat dalam bidang keamanan informasi diperlukan adanya pemeliharaan serta peningkatan ketersediaan, keutuhan, dan kerahasiaan data / informasi dalam layanan publik ;
b. bahwa untuk melaksanakan kegiatan sebagaimana dimaksud dalam

Revitalisasi JabarProv-CSIRT Tahun 2018 :

1. Penetapan Struktur Organisasi JabarProv-CSIRT Tahun 2018
2. Perbaikan Fungsi dan Uraian Tugas
3. Penyusunan Alur Kerja
4. Pembahasan Program Kerja Tahun 2018 - 2019

Insiden Keamanan Informasi di Pemerintah Daerah Provinsi Jawa Barat

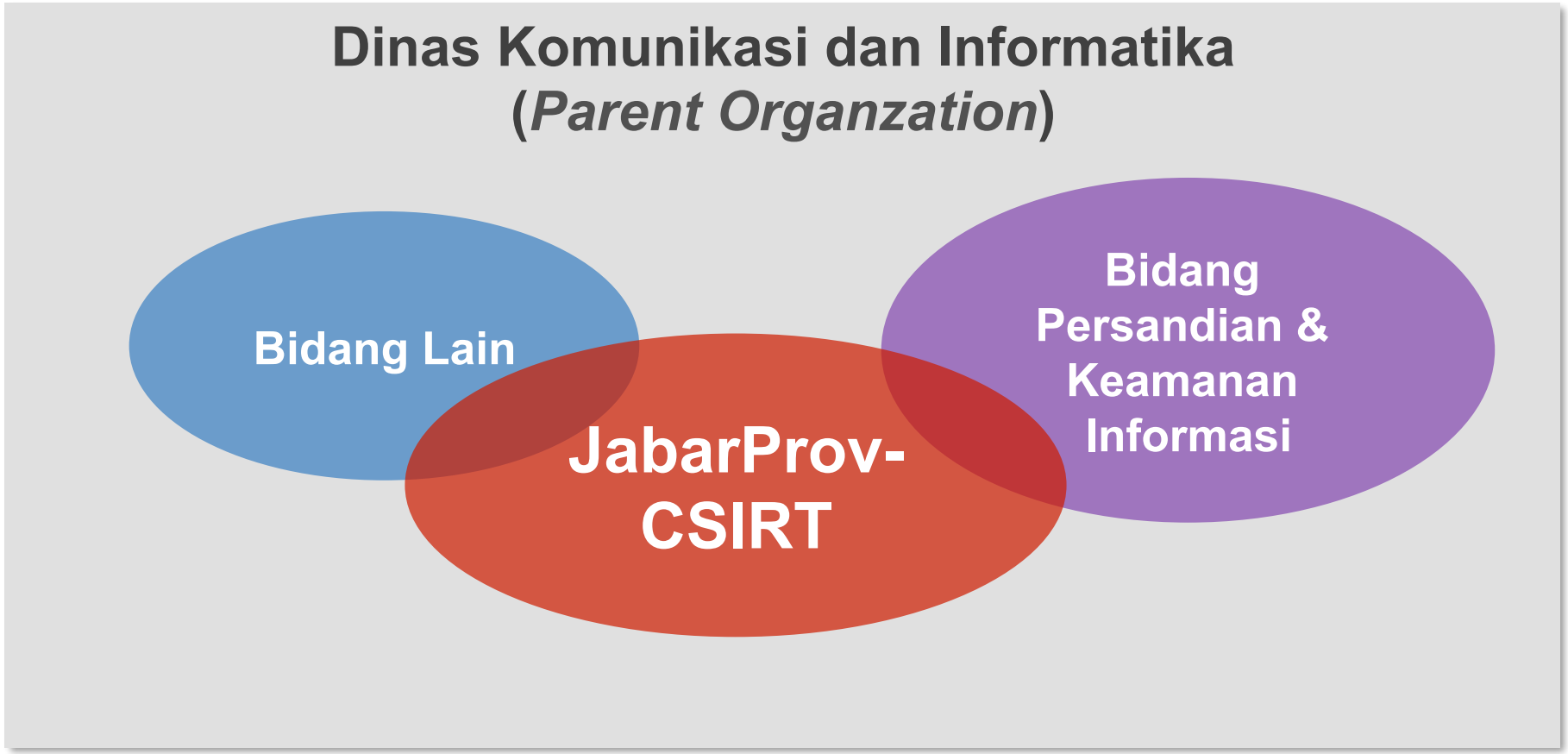
Terdapat sekitar **243 kasus** terjadinya **defacement** pada situs pemerintah provinsi Jawa Barat (domain : jabarprov.go.id)

pada tahun 2018 tercatat sudah terjadi insiden defacement sebanyak **11 website** dengan **domain jabarprov.go.id :**

1. brsmp.dissos.jabarprov.go.id
2. inspektorat.jabarprov.go.id
3. rsudalihsan.jabarprov.go.id
4. simpeg-guru.jabarprov.go.id
5. hibahbansos.jabarprov.go.id
6. dss.jabarprov.go.id
7. bpbd.jabarprov.go.id
8. simpel.sda.jabarprov.go.id
9. diskanlaut.jabarprov.go.id
10. bpstw.dissos.jabarprov.go.id
11. bpkaa.dissos.jabarprov.go.id

Data dari http://zone-h.org

Kedudukan JabarProv-CSIRT di internal Dinas Kominfo Jabar



SOC & JabarProv-CSIRT

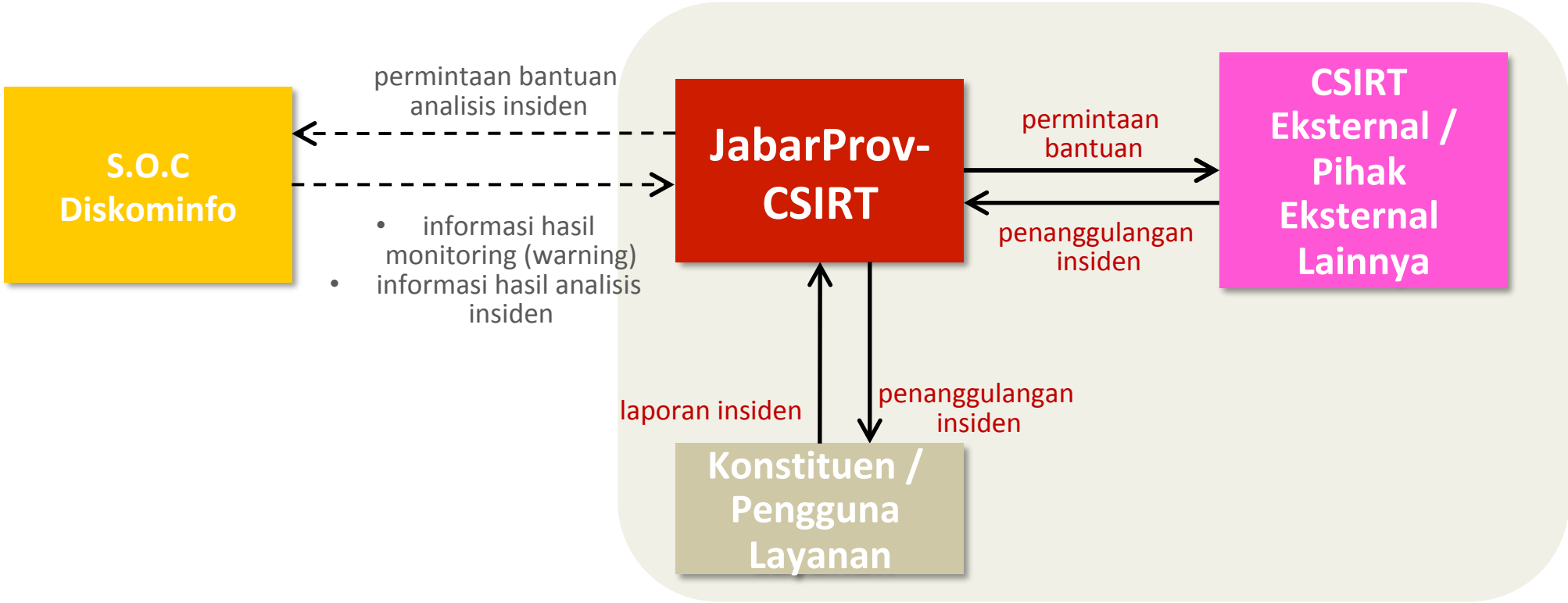
SOC
(pengawasan, perlindungan, dan penanggulangan insiden keamanan infomasi)

JabarProv-CSIRT
(penanggulangan insiden keamanan informasi)

- Fungsi JabarProv-CSIRT merupakan pengerucutan dari fungsi SOC dimana JabarProv-CSIRT spesifik mengelola penanggulangan insiden keamanan informasi

- Pengelola JabarProv-CSIRT merupakan perluasan dari Pengelola SOC untuk keperluan koordinasi antar pihak terkait dalam penanggulangan insiden keamanan informasi

Tata Kelola JabarProv-CSIRT



Saat terjadi insiden keamanan informasi , jika diperlukan, JabarProv-CSIRT berkoordinasi dengan CSIRT lainnya untuk meminta bantuan atau mencegah skala insiden meluas

Visi dan Misi JabarProv-CSIRT

VISI

- Terciptanya sistem keamanan informasi yang handal di lingkungan Pemerintah Daerah Provinsi Jawa Barat

MISI

- Membangun pusat pencatatan, pelaporan, dan penanggulangan insiden keamanan informasi di lingkungan Pemerintah Daerah Provinsi Jawa Barat
- Membangun lingkungan dan membuat skema untuk mengurangi kerusakan/ kerugian insiden keamanan informasi pada konstituennya
- Meningkatkan kesadaran pentingnya keamanan informasi bagi sumber daya manusia di lingkungan Pemerintah Daerah Provinsi Jawa Barat

Ruang Lingkup

LEVEL LAYANAN

- Layanan Reaktif, dipicu oleh suatu kejadian atau berdasarkan permintaan.

JENIS INSIDEN

- Jenis insiden yang ditangani mencakup Spam, Phising / Spoofing, Malware, Network Incident (Brute Force, DDoS, Deface, dsb).

KONSTITUEN

- Konsituten (pengguna layanan) adalah semua Perangkat Daerah di Lingkungan Pemerintah Daerah Provinsi Jawa Barat.

PRIORITAS

- Perangkat Daerah yang memberikan layanan publik.

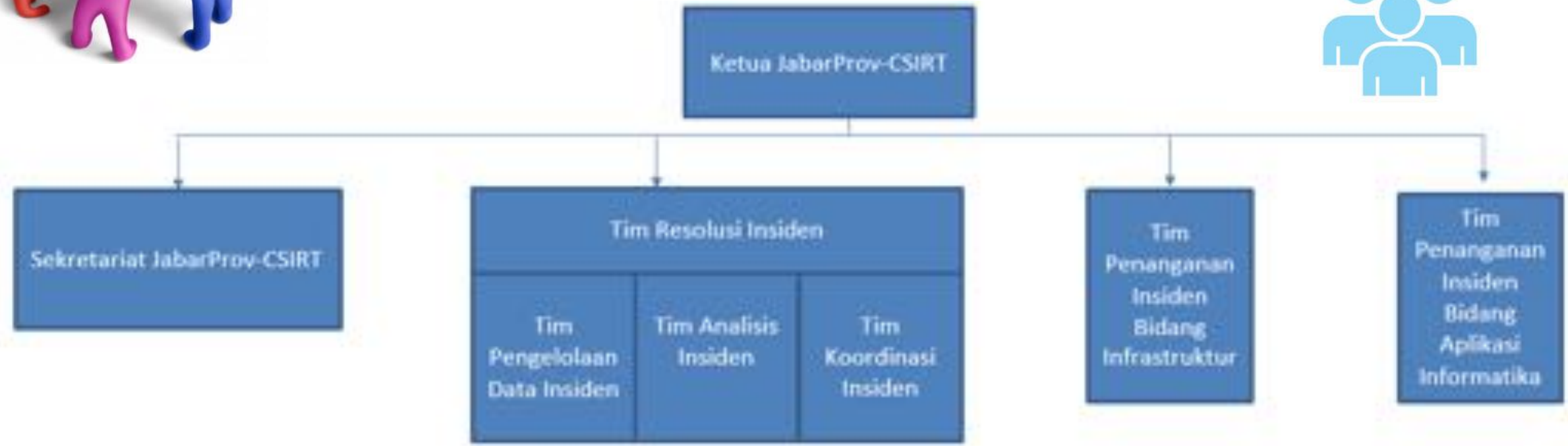
Layanan Reaktif JabarProv-CSIRT

Kewaspadaan dan Peringatan

Penanggulangan Insiden

- Analisis Insiden
- Respon Insiden
- Koordinasi untuk Merespon Insiden

Organisasi JabarProv-CSIRT



Keputusan Kepala Dinas Komunikasi dan Informatika Provinsi Jawa Barat Nomor : 046/Kep. 1246/Diskominfo, Tanggal : 23 Juli 2018, Tentang *Computer Security Incident Response Team* Provinsi Jawa Barat (JabarProv-CSIRT)

Tugas dan Fungsi JabarProv-CSIRT

- Memberikan kesadaran keamanan informasi di instansi Pemerintah Daerah Provinsi Jawa Barat
- Menyediakan layanan respon bila terjadi serangan
- Melakukan identifikasi/analisis suatu serangan
- Mengarsipkan semua serangan yang terjadi
- Penghubung bila terjadi insiden keamanan informasi

Uraian Tugas Tim JabarProv-CSIRT

Tim Pengelolaan Data Insiden

- Menerima, mendokumentasikan, dan meneruskan laporan insiden dari pengguna layanan TIK apabila terjadi insiden kemanan informasi pada Pemprov Jabar

Tim Analisis Data Insiden

- Melakukan identifikasi, investigasi, dan analisis terhadap insiden yang terjadi
- Memberikan rekomendasi solusi insiden

Tim Koordinasi Insiden

- Mengkoordinasikan dan memfasilitasi penanganan insiden keamanan informasi baik di antara Tim Internal Jabarprov-CSIRT maupun dengan pihak lain yang mungkin dilibatkan: komunitas / lembaga / CSIRT / pihak eksternal lainnya, apabila diperlukan

Tim Penanganan Insiden

- Menangani insiden kemanan informasi di Bidang Infrastruktur TIK, Aplikasi Informatika, dan Data Elektronik yang terjadi pada Pemerintah Provinsi Jawa Barat yang mampu ditangani oleh Tim

SDM Penunjang JabarProv-CSIRT

NO	SERTIFIKAT/PELATIHAN	JUMLAH SDM	TAHUN
1	CISM (Information Security Manager)	18 orang	2017
2	TOGAF (The Open Group Architectural Framework)	5 orang	2017
3	ITIL (Information Technology Infrastructure Library)	7 orang	2017
4	CAPM (Certified Associate in Project Management)	10 orang	2017
5	CDCP (Certified Data Centre Professional)	6 orang	2017
6	ISO 27001 : 2013 (Information Security Management Standard)	10 orang	2017

No	Kegiatan	Pelaksana					Output	Keterangan
		Helpdesk Dinas Kominfo	Tim Pengelolaan Data	Tim Analisis	Tim Koordinasi	Tim Penanganan / CSIRT / Pihak Eksternal Lainnya		
1	Menerima laporan insiden, melakukan validasi, registrasi, dan meneruskan laporan ke JabarProv-CSIRT						Isian Incident Report Form	Validasi dilakukan untuk menilai apakah benar terjadi insiden
2	Menerima laporan insiden dan meneruskan laporan ke Tim Analisis						Input data ke aplikasi pelaporan insiden	
3	Melakukan incident triage, investigasi / analisis insiden, dan memberikan rekomendasi untuk ditindaklanjuti oleh Tim Koordinasi						Rekomendasi Tim Analisis	Incident Triage dilakukan untuk menilai apakah insiden sesuai dengan skala dan prioritas ruang lingkup JabarProv-CSIRT
4	Berkoordinasi dengan Tim Penanganan internal JabarProv-CSIRT atau CSIRT / pihak eksternal lainnya, apabila diperlukan, sesuai rekomendasi Tim Analisis					perlu	Terjalinnya kontak dengan Tim Penanganan Insiden atau pihak eksternal yang diperlukan	
5	Penanganan insiden dan/atau pemberian rekomendasi oleh Tim Penanganan internal JabarProv-CSIRT atau CSIRT / pihak eksternal lainnya				tidak perlu		Laporan penanganan insiden dan/atau rekomendasi	
6	Menerima, mengkompilasi, dan meneruskan rekomendasi dan/atau laporan penanganan insiden						Laporan dan/atau Rekomendasi JabarProv-CSIRT	
7	Menerima dan meneruskan Laporan dan/atau Rekomendasi JabarProv-CSIRT ke Helpdesk						Laporan dan/atau Rekomendasi JabarProv-CSIRT (tercatat di Helpdesk)	
8	Menerima dan meneruskan Laporan dan/atau Rekomendasi JabarProv-CSIRT ke pemohon / owner aplikasi						Laporan lanjutan atau Laporan ditutup	Memasuki masa autoresolved (3 hari). Laporan lanjutan akan ditangani dalam masa ini. Setelah masa autoresolved selesai maka status laporan insiden akan ditutup.
9	Mendokumentasikan insiden dan menutup status insiden						Dokumentasi insiden	
10	Menutup status laporan						Status laporan ditutup	

Standard Operating Procedure

Program Kerja JabarProv-CSIRT 2018 - 2019

NO	KEGIATAN	BULAN KE -											
		1	2	3	4	5	6	7	8	9	10	11	12
1.	Penyusunan Kebijakan dan Regulasi Penanggulangan Insiden												
2.	Penyusunan Pedoman Standar dan Teknik Penanggulangan Insiden												
3.	Pengadaan Sarana dan Prasarana Pendukung Penanggulangan Insiden												
4.	Peningkatan Kapasitas SDM :												
	a. Internal (Bimtek, Sertifikasi)												
	b. Perangkat Daerah / Kab. / Kota (Bimtek, Security Awareness)												
5.	Simulasi Penanggulangan Insiden												
6.	Koordinasi dengan Pihak Eksternal (CSIRT Lainnya / BSSN)												
7.	Rapat Periodik												

JabarProv-CSIRT Flagship Program

Pengadaan Perangkat Penanganan Insiden

Penyusunan Standar dan Teknik Penanganan Insiden

Penyusunan Kebijakan & Regulasi Penanganan Insiden

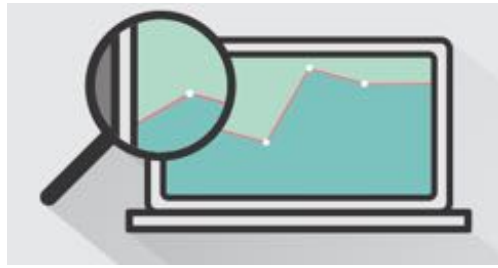
Peningkatan Kesadaran Keamanan Informasi

Penguatan SDM Keamanan Informasi

Contoh Penanganan Insiden JabarProv-CSIRT Tahun 2018

BKD Prov. Jabar menyampaikan laporan insiden keamanan informasi (website defacement)

Laporan diterima oleh JabarProv-CSIRT



Insiden defacement dianalisa oleh JabarProv-CSIRT

Penyebab insiden ditemukan

JabarProv-CSIRT melakukan penanganan teknis agar insiden tidak meluas

JabarProv-CSIRT mengirim surat rekomendasi ke BKD untuk perbaikan aplikasi agar insiden tidak terulang kembali

~ Terima Kasih ~

JabarProv-CSIRT

Alamat *: Kantor Dinas Komunikasi dan Informatika Provinsi Jawa Barat, Jl. Taman Sari No 55 Bandung 40132*

Email Aduan JabarProv-CSIRT *: abuse@csirt.jabarprov.go.id*