



**SOSIALISASI PEMBENTUKAN
TIM TANGGAP INSIDEN SIBER
(COMPUTER SECURITY INCIDENT
RESPONSE TEAM)
MPR-CSIRT**



SEJARAH CSIRT



CSIRT adalah sebuah organisasi atau tim yang bertanggungjawab untuk menerima, meninjau dan menanggapi laporan dan aktivitas insiden keamanan siber. Tim ini bentuk dengan tujuan untuk melakukan penyelidikan komprehensif dan melindungi sistem atau data atas insiden keamanan siber yang terjadi pada organisasi. Selain itu CSIRT juga dibentuk untuk melakukan pencegahan insiden dengan cara terlibat aktif pada penilaian dan deteksi ancaman, perencanaan mitigasi, dan tinjauan atas arsitektur keamanan informasi organisasi.

PERETASAN SITUS MPR.GO.ID

Tercatat beberapa kali insiden terhadap website MPR RI



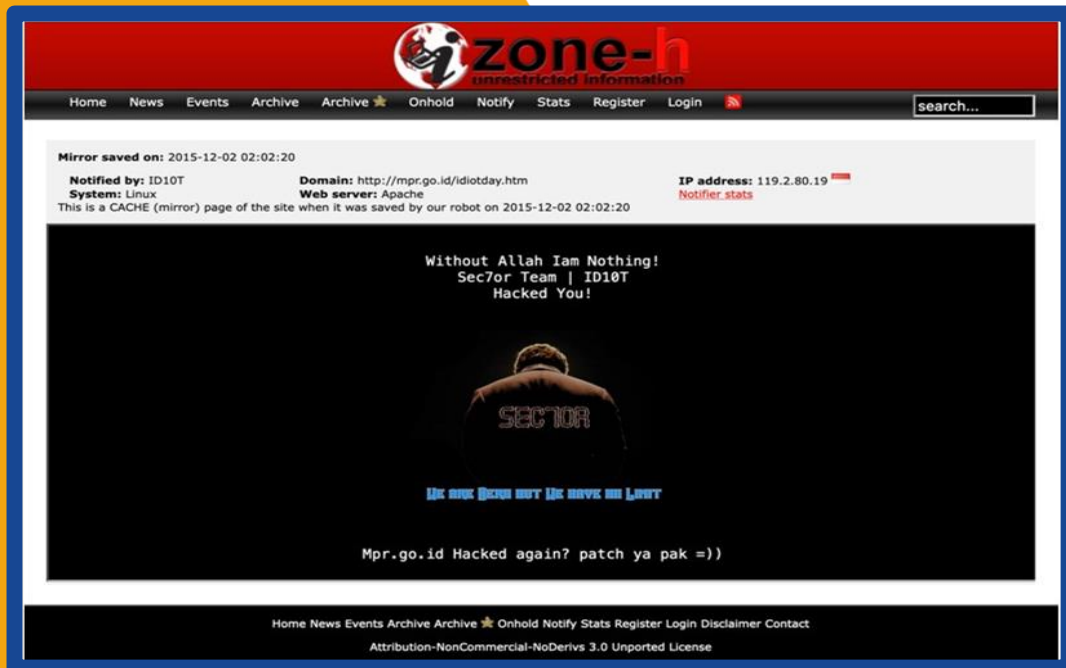
23 Oktober 2011



30 November 2014

PERETASAN SITUS MPR.GO.ID (2)

Tercatat beberapa kali insiden terhadap website MPR RI




2 Desember 2015



10 Mei 2017

PERETASAN SITUS MPR.GO.ID (unpublished)





Home News Events Archive Archive ★ Onhold Notify Stats Register Login

NOTIFIER DOMAIN

Special defacements only Fulltext/Wildcard Onhold (Unpublished) only

Date :

Total notifications: 7 of which 7 single ip and 0 mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

We don't accept notifications through email, IP address notifications, notifications with fake and/or created subdomains by notifier or with wrong attack methods selected.

Time	Notifier	H	M	R	L	★ Domain	OS	View
2022/09/21	Black_X12					★ csirt.mpr.go.id/root.php	Linux	mirror
2020/12/23	MrL00L	H		R		★ ppid.mpr.go.id	Linux	mirror
2020/05/13	BCA-X666X			R		★ mpr.go.id/sekretariat_jendral/...	Unknown	mirror
2019/03/27	tes	H		R		★ mpr.go.id	Unknown	mirror
2018/03/12	UmbrellaTikTok	H		R		★ mpr.go.id	Linux	mirror
2016/12/09	PhantomGhost	H		R		★ mpr.go.id	Linux	mirror
2016/01/14	Benny-x207	H				★ pdf.mpr.go.id	Linux	mirror

1

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified **anonymously** to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. [Read more](#)

URGENSI CSIRT

- **Mengelola informasi yang relevan dengan insiden.**
 - Berbagi informasi keamanan serta manajemen informasi keamanan yang terpusat.
 - Penyederhanaan pengambilan keputusan untuk respon insiden.
- **Menyediakan pusat poin of contact.**
 - Pihak ketiga tepercaya yang mengkomunikasikan informasi insiden secara langsung.
 - Realisasi konsolidasi informasi dari luar.
- **Membangun hubungan tepercaya yang diperlukan untuk merespon.**
 - Meningkatkan konten informasi yang dibutuhkan untuk respon insiden.
 - Siap untuk merespon insiden.

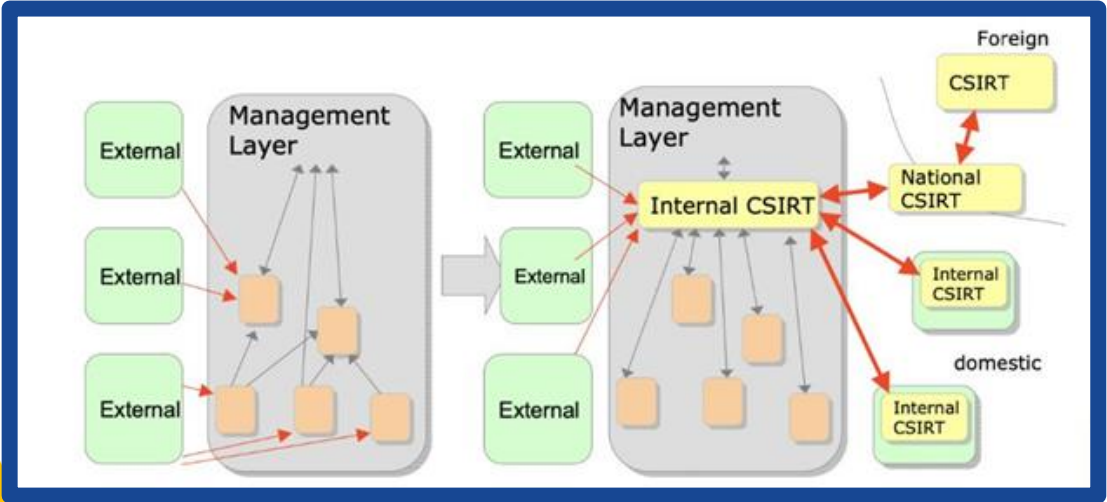
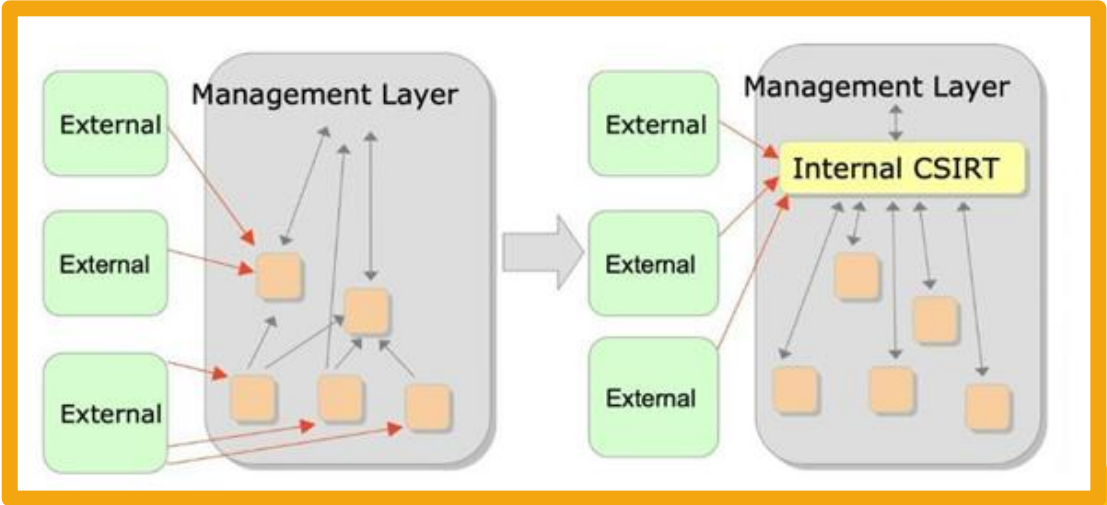


DASAR HUKUM

PEMBENTUKAN CSIRT

1. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
2. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik
3. Peraturan Presiden Nomor 18 Tahun 2020 tentang Rencana Pemerintah Jangka Menengah Nasional (RPJMN) 2020-2024. BSSN diamanatkan untuk membentuk CSIRT sektor Pemerintah sebanyak 121 CSIRT yang dilaksanakan selama 5 (lima) tahun
4. Surat Kepala Badan Siber dan Sandi Negara Nomor T.01 /KABSSN/PP.01.07/01/2022 tanggal 4 Januari 2022 perihal Penunjukkan Instansi Pemerintah Pusat dalam Program Pembentukan CSIRT Tahun 2022.
5. Keputusan Sekretaris Jenderal MPR RI Nomor 179B tanggal 1 Agustus 2022 tentang TIM PENANGGULANGAN DAN PEMULIHAN INSIDEN SIBER (COMPUTER SECURITY INCIDENT RESPONSE TEAM) Sekretariat Jenderal MPR RI

MANAGEMENT LAYER





Kompetensi Dasar Staf CSIRT

Personal Skills

- ❖ Communication
- ❖ Presentation Skills
- ❖ Diplomacy
- ❖ Ability to Follow Policies and Procedures
- ❖ Team Skills
- ❖ Integrity
- ❖ Knowing One's Limits
- ❖ Coping with Stress
- ❖ Problem Solving
- ❖ Time Management

Technical Skills

Technical Foundation Skills

- ❖ The Internet
- ❖ Security Principles
- ❖ Security Vulnerabilities/Weakness
- ❖ Risk
- ❖ Network Protocol
- ❖ Network Applications and Services
- ❖ Network Security Issues
- ❖ Host/System Security Issues
- ❖ Malicious Code
- ❖ Programming Skills

Incident Handling Skills

- ❖ Local Team Policies and Procedures
- ❖ Understanding/Identifying Intruder Techniques
- ❖ Incident Analysis
- ❖ Maintenance of Incident Records



SUMBER DAYA MANUSIA

KONDISI SAAT INI

Bagian Sistem Informasi dan Data (BSID) terdiri dari 10 orang Pegawai dengan rincian sebagai berikut :

- 1 (satu) orang Kepala Bagian
- 2 (dua) orang Kepala Sub Bagian
- 4 (empat) orang PNS
- 3 (tiga) orang PPNPN

KONDISI YANG DIHARAPKAN

Bagian Sistem Informasi dan Data (BSID) terdiri dari 10 orang Pegawai untuk pelaksanaan tugas fungsi yang sudah berjalan yaitu

- 1 (satu) orang Kepala Bagian
- 2 (dua) orang Kepala Sub Bagian
- 4 (empat) orang PNS
- 3 (tiga) orang PPNPN

Dengan dibentuknya CSIRT , minimal ada tambahan personal dengan Kompetensi sebagai berikut :

- 1 (satu) orang Analis Cyber Security
- 1 (satu) orang Pentester
- 1 (satu) orang Fullstack Developer

FUNGSI CSIRT

1. **Defence**, melindungi infrastruktur kritis;
2. **Monitoring**, menganalisis anomali dengan berbagai pola terdefinisi dan pola tak terdefinisi;
3. **Intercepting**, yakni mengumpulkan konten spesifik atau disebut targeted content;
4. **Surveillance**, mengamati dan menganalisis aktivitas yang dicurigai dan informasi yang berubah dalam sistem;
5. **Mitigating**, mengendalikan kerusakan dan menjaga ketersediaan serta kemampuan layanan tersebut;
6. **Remediation**, membuat solusi untuk mencegah kegiatan yang berulang ulang dan mempengaruhi sistem; dan
7. **Offensive**, upaya pencegahan atau perlawanan dengan menyerang balik seperti Cyber Army serta kemampuan untuk menembus sistem keamanan.

APA YANG DILAKUKAN CSIRT

UMUM

- Menyediakan satu titik kontak untuk melaporkan masalah/insiden siber yang terjadi di lokal;
- Mengidentifikasi dan menganalisis apa yang telah terjadi termasuk dampak dan ancamannya;
- Mencari solusi dan strategi mitigasi;
- Berbagi opsi respons, informasi, dan pelajaran yang dipetik;
- Membangun kesadaran dan kapasitas di dalam dan di luar organisasi.

Tujuan CSIRT:

- Meminimalkan dan mengendalikan kerusakan;
- Memberikan atau membantu dengan respons dan pemulihan yang efektif;
- Membantu mencegah kejadian di masa depan.



LAYANAN CSIRT



Terdiri atas:

1. Pemberian peringatan terkait keamanan siber; dan
2. Pengelolaan Insiden Siber.

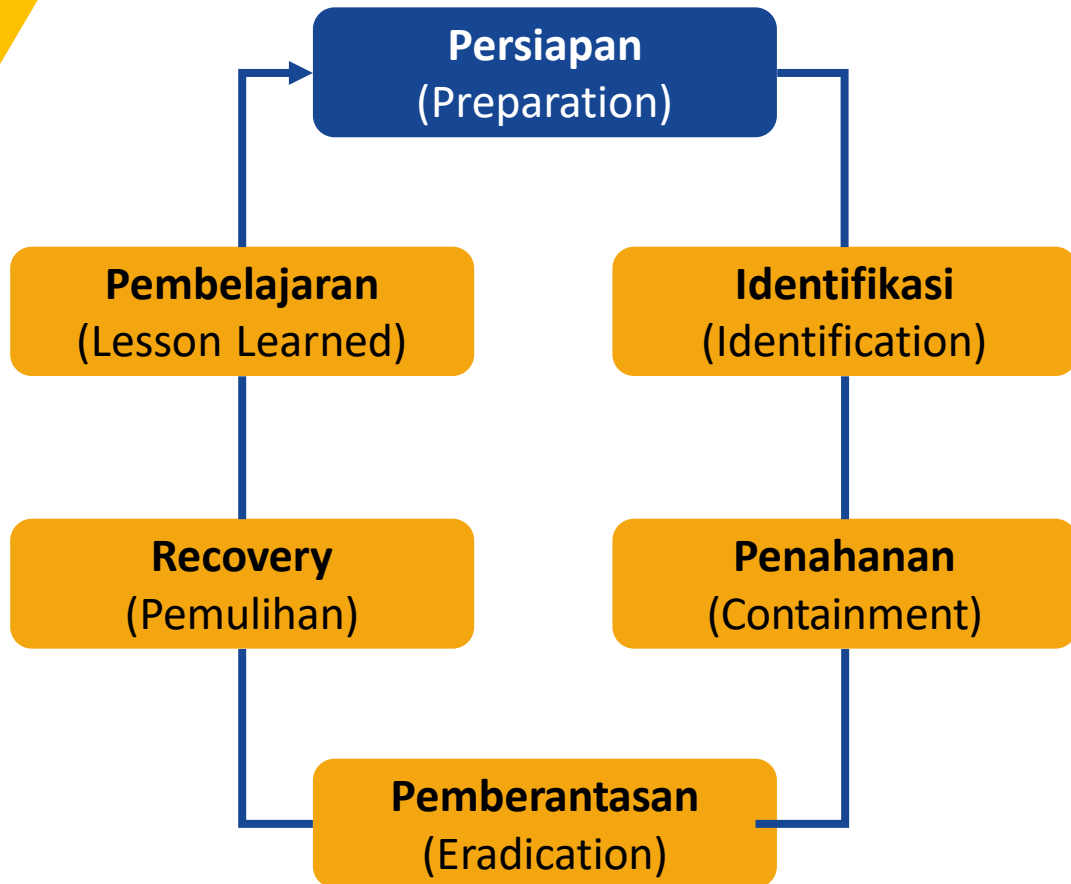
[Pasal 13 ayat (1)]

Terdiri atas:

1. Penanganan kerentanan sistem elektronik; **REAKTIF**
2. Penanganan artefak digital; **REAKTIF**
3. Pemberitahuan hasil pengamatan potensi ancaman; **PROAKTIF**
4. Pendeteksian serangan; **PROAKTIF**
5. Analisis risiko keamanan siber; **LAYANAN PENINGKATAN KESIAPAN PENANGANAN INSIDEN SIBER**
6. Konsultasi terkait kesiapan penanganan Insiden Siber; dan/atau **LAYANAN PENINGKATAN KESIAPAN PENANGANAN INSIDEN SIBER**
7. Pembangunan kesadaran dan kepedulian terhadap keamanan siber. **LAYANAN PENINGKATAN KESIAPAN PENANGANAN INSIDEN SIBER**

[Pasal 14 ayat (1)]

FASE INSIDEN RESPON



- **PERSIAPAN (PREPARATION)** → Tim (internal, eksternal, role, kepemilikan sistem, penentuan layanan, jalur komunikasi alternative, partisipasi dalam program peningkatan kapasitas)
- **IDENTIFIKASI (IDENTIFICATION)** → apakah insiden? Bagaimana ruang lingkupnya (dampak dan urgensi)? Identifikasi kategori insiden, tentukan SLA
- **PENAHANAN (CONTAINMENT)** → membatasi kerusakan dan mencegah terjadinya kerusakan lebih lanjut.
- **PEMBERANTASAN (ERADICATION)** → pemindahan dan pemulihan dari sistem yang terkena dampak
- **RECOVERY (PEMULIHAN)** → mengembalikan sistem yang terdampak insiden
- **PEMBELAJARAN YANG DIDAPAT (LESSON LEARNED)** → dokumentasi insiden dan tindakan penanganan yang dilakukan yang mungkin dapat dijadikan sebagai acuan apabila terjadi insiden yang serupa.

BEBERAPA HAL YANG TELAH DISIAPKAN TERKAIT RENCANA LAUNCHING MPR CSIRT

- Surat keputusan Sekretaris Jenderal MPR RI Tentang Pembentukan Tim CISRT
- Profil CISRT dalam format RFC 2350
- Surat Pernyataan kesediaan Menjadi Narahubung (POC)
- Surat Pernyataan kesediaan berbagi informasi tentang penanganan Insiden Keamanan Siber
- Dokumen Daftar Sumber Daya Penyelenggara CSIRT Form aduan siber, formulir penanganan insiden dan format laporan penanganan insiden
- Video Profil CSIRT yang akan ditampilkan saat pelaksanaan Launching CISRT

PC ATAU SERVER YANG DIGUNAKAN UNTUK OPERASIONAL CSIRT

- Media Publikasi Layanan CSIRT dalam bentuk Website dengan spesifikasi minimal 8 GB RAM, 100 GB Harddisk, dan 4 Core CPU;
- Media Layanan Aduan Siber dan Pelaporan Insiden dengan spesifikasi minimal 8 GB RAM, 200 GB Harddisk, dan 8 Core CPU;
- Sistem Monitoring (IDS/IPS) dengan spesifikasi minimal 16 GB RAM, 500 GB Harddisk, dan 8 Core CPU



RANGKAIAN KEGIATAN YANG DI IKUTI SETJEN MPR TERKAIT CSIRT

Latihan kesiapsiagaan teknis insiden keamanan siber (CYBER SECURITY EXERCISE TECHNICAL) SEKTOR PEMERINTAH PUSAT TAHUN 2021, tanggal 10 s.d. 12 November 2021 di Daerah Istimewa Yogyakarta (Juara II)

Rapat Koordinasi lanjutan dengan BSSN Rencana Pembentukan MPR CSIRT pada tanggal 9 Maret 2022 di Ruang Rapat Samithi Gedung Nusantara V

Workshop Peduli Keamanan Informasi (PEDULI KAMI) pada Sektor Pemerintah Tahun 2022, 22 s.d. 24 Maret 2022, di Kota Bogor

Kegiatan Cyber Security Exercise Table Top di Auditorium BSSN, Tanggal 7 Juli 2022, Kota Depok (Juara I)

Kegiatan Pertemuan Tahunan CSIRT Organisasi Sektor Pemerintah Pusat Tahun 2022, Tanggal 4 Agustus 2022 di Tangerang

Workshop Pengelolaan Manajemen Risk Appetite dan Asistensi Penilaian Cyber Security Maturity (CSM) Tahun 2022, 10 Agustus 2022, secara daring

RANGKAIAN KEGIATAN YANG DI IKUTI SETJEN MPR TERKAIT CSIRT (2)

Penyelenggaraan Pelatihan Sertifikasi EC-Council Certified Incident Handler (ECIH) dan Linux Networking and Security for Ministry and Province CSIRT Registered in Badan Siber dan Sandi Negara Paket II T.A. 2022, tanggal 8 s.d. 18 Agustus 2022 secara daring

Penyelenggaraan Pelatihan Sertifikasi EC-Council Certified Ethical Hacker (CEH) dan Threat Hunting for Ministry and Province CSIRT Registered in Badan Siber dan Sandi Negara Paket II T.A. 2022, Tanggal 22 Agustus s.d. 2 September 2022

Rapat Koordinasi Tindak Lanjut Pembentukan CSIRT sebagai Program Prioritas Nasional Tahun 2022, tanggal 7 September 2022, di Jakarta

Kegiatan Kesiapsiagaan Teknis Penanganan Insiden Keamanan Siber Sektor Pemerintah Pusat (Cyberdrill Exercise).
Bandung, 20-22 September 2022

Workshop Pengelolaan CSIRT Pemerintah Pusat.
Bandung, 22-24 September 2022



EVALUASI OPERASIONAL CSIRT

- CSIRT perlu melakukan review terhadap dokumen RFC-2350
- Update website CSIRT
- Update kontak CSIRT
- Review pelaksanaan layanan
- Review sumber daya yang dimiliki (SDM, perangkat, sistem, form aduan, form penanganan)



WEB CSIRT

MPR-CSIRT

Ini Profil baru, welcome to Website MPR-CSIRT

BSSN menyediakan template *Website* sebagai media publikasi CSIRT, tools (*open source*) baik *tools* untuk aduan/pelaporan siber maupun untuk system *monitoring* beserta dengan dokumen petunjuk instalasinya yang dapat diimplementasikan oleh masing-masing Instansi

KESALAHAN UMUM DALAM CSIRT

- Tim CSIRT melakukan insiden response hingga perbaikan aplikasi
- Insiden terjadi karena kegagalan Tim CSIRT melindungi
- Sudah ada Tim CSIRT/Keamanan (semua masalah akan terselesaikan)
- Rencana tanggap insiden hanya digunakan saat terjadi insiden
- Tim CSIRT tidak membangun komunikasi dengan unit lain atau orang yang tepat
- Tidak ada data yang diperlukan Tim CSIRT untuk menganalisis insiden
- Skill dari anggota Tim CSIRT tidak dipelihara
- Pengguna di dalam organisasi tidak memahami perannya dalam keamanan
- Organisasi tidak memiliki identifikasi asset dan penilaian resiko keamanan terkait aset





MPR CSIRT
Gedung Bharana Graha II Lantai II
csirt@mpr.go.id
<https://csirt.mpr.go.id/>