Sosialisasi CSIRT

Riki Arif Gunawan

Kasubdit Teknologi Kemanan Informasi
Direktorat Keamanan Informasi
Kementerian Komunikasi dan Informatika

Agenda

- Apakah Informasi?
- Apakah Keamanan Informasi?
- Apakah Risiko
- Apakah Peran CSIRT
- Struktur CSIRT Nasional

Apakah Informasi?

"Information is an asset which, like other **important business assets**, has value to an organization and consequently needs to be suitably **protected**"

BS ISO 27002:2005

Informasi bisa ...

- Dibuat
- Disimpan
- Dihancurkan
- Diproses
- Dikirimkan
- Digunakan
- Rusak
- Hilang
- Dicuri

Jenis Informasi

- ➢Dicetak atau ditulis pada kertas (hard copy)
- ➢Disimpan secara elektronik (softcopy)
- ➢Informasi yang dikirim melalui pos atau elektronik
- ➢Dalam bentuk video perusahaan
- ➢Ditampilkan pada website
- ➢Verbal – pembicaraan dalam rapat dll.

'…Whatever form the information takes, or means by which it is shared or stored, ***it should always be appropriately protected****'*

(BS ISO 27002:2005)

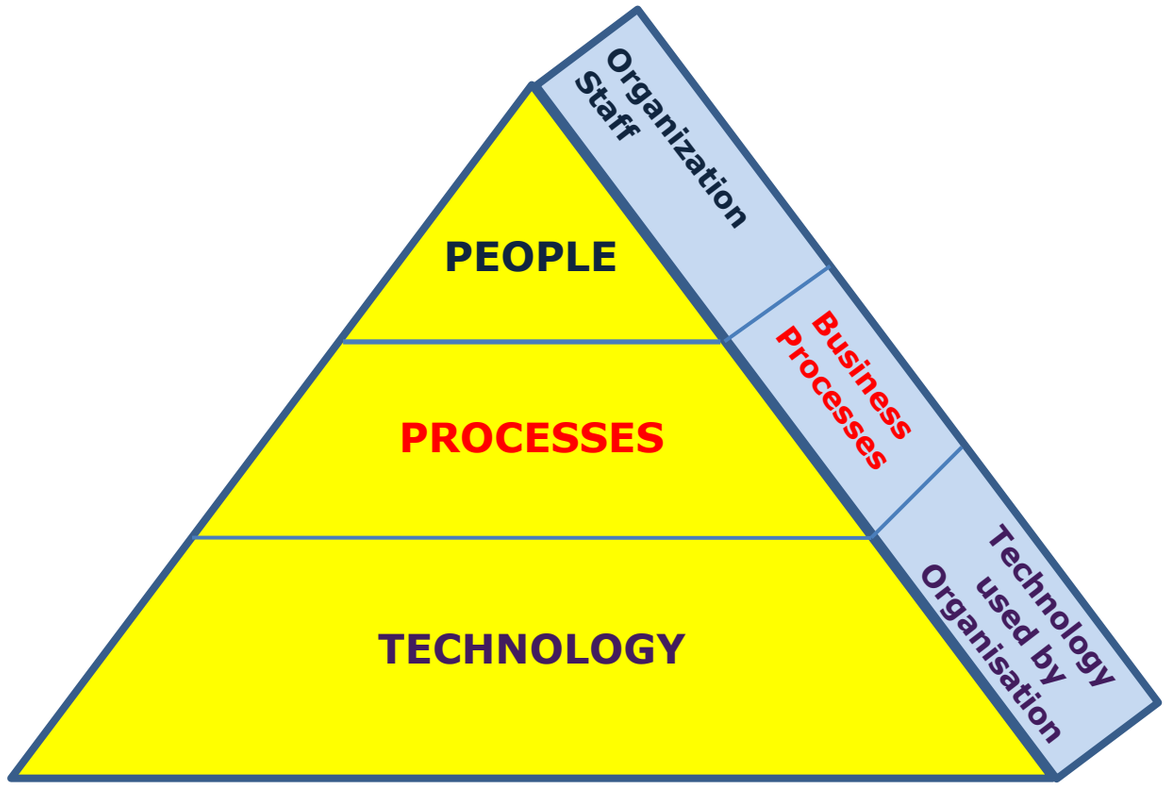
Information Security

- The quality or state of being secure to be free from danger
- Security is achieved using several strategies
- Security is achieved using several strategies simultaneously or used in combination with one another
- Security is not something you buy, it is something you do

Information Security

- The architecture where an integrated combination of appliances, systems and solutions, software, alarms, and vulnerability scans working together
- Monitored 24x7
- Having **P**eople, **P**rocesses, **T**echnology, policies, procedures,
- Security is for **PPT** and not only for appliances or devices

Komponen Keamanan Informasi



Information Security

1. Protects information from a range of threats
2. Ensures business continuity
3. Minimises financial loss
4. Optimises return on investments
5. Increases business opportunities

Business survival depends on information security.

Info Sec Survey

- Information Security is “Organizational Problem” rather than “IT Problem”
- More than 70% of Threats are Internal
- More than 60% culprits are First Time fraudsters
- Biggest Risk : People
- Biggest Asset : People
- Social Engineering is major threat
- More than 2/3rd express their inability to determine “Whether my systems are currently compromised?”

What is risk

Risk: A possibility that a threat exploits a vulnerability in an asset and causes **damage** or **loss** to the asset.

Threat: Something that can **potentially cause damage** to the organisation, IT Systems or network.

Vulnerability: A **weakness** in the organization, IT Systems, or network that can be exploited by a threat.

Risk = Threat x Vulnerability

Threat Sources

Source	**Motivation**	**Threat**
External Hackers	Challenge Ego Game Playing	System hacking Social engineering Dumpster diving
Internal Hackers	Deadline Financial problems Disenchantment	Backdoors Fraud Poor documentation
Terrorist	Revenge Political	System attacks Social engineering Letter bombs Viruses Denial of service
Poorly trained employees	Unintentional errors Programming errors Data entry errors	Corruption of data Malicious code introduction System bugs Unauthorized access

Information Attributes

ISO 27002:2005 defines Information Security as the preservation of:

- **Confidentiality**

Ensuring that information is accessible only to those authorized to have access

- **Integrity**

Safeguarding the accuracy and completeness of information and processing methods

- **Availability**

Ensuring that authorized users have access to information and associated assets when required

Security breaches leads to…

- **Reputation loss**
- **Financial loss**
- **Intellectual property loss**
- **Legislative Breaches leading to legal actions (Cyber Law)**
- **Loss of customer confidence**
- **Business interruption costs**

LOSS OF GOODWILL

Pentingnya Menjaga Informasi

Kebutuhan Bersama/ Pimpinan/Organisasi

Membentuk Tim/Organisasi Keamanan Informasi

Tim Keamanan Informasi

Menyiapkan Dokumen dan SOP

Risk Manajemen

BCP dan DRP

Perbaikan

Evaluasi Implementasi

Training dan Implementasi

Tim CSIRT Instansi

Alasan Pendirian CSIRT

- Infrastruktur keamanan yang terbaikpun tidak dapat menjamin serangan tidak akan terjadi.
- Bila insiden terjadi, maka institusi bergerak cepat untuk merespon secara efektif dengan memimalisasi kerusakan dan mengurangi biaya recovery.
- Untuk melindungi kejadian-kejadian yang tidak diinginkan di masa depan dengan mengatur strategi keamanan, berbagi informasi untuk update pengetahuan dan berkolaborasi dengan CSIRT yang lain.
- Fokus kepada pencegahan kerentanan keamanan, melakukan mitigasi dan memastikan pemenuhan/pencapaian regulasi dan kebijakan keamanan institusi.

Mengapa butuh CSIRT?

Saat insiden cyber terjadi dan menyebar, maka perlu tindakan segera seperti :

- Secara efektif mendeteksi dan mengidentifiaksi segala macam aktivitas.
- Melakukan mitigasi dan merespons secara strategis.
- Membangun saluran komunikasi yang dapat dipercaya.
- Memberikan peringatan dini kepada masyarakat dan konstituen tentang dampak yang akan dan sudah terjadi.
- Memberitahu pihak yang berkepentingan tentang masalah yang potensial di komunitas keamanan dan internet.
- Berkoordinasi dalam meresponse insiden.
- Berbagi data dan informasi tentang segala aktivitas dan melakukan korespondensi untuk response segala solusi kepada konstituen.
- Melacak dan memonitor informasi untuk menentukan tren dan strategi jangka panjang.

Lingkup Pekerjaan CSIRT

- Menyediakan satu pintu untuk kontak insiden.
- Melakukan identifikasi, analisis, dampak dari ancaman/insiden.
- Penelitian, mitigasi, rencana strategi dan pelatihan.
- Berbagi pengalaman, informasi dan belajar/ mengajar.
- Kesadaran, membangun kapasitas, jejaring.
- Merespon, mengontrol kerusakan, recovery, meminimalisir resiko dan manajemen resiko, pencegahan dan pertahanan.

Macam-macam CSIRT

- **Internal CSIRT:** menyediakan layanan penanganan insident kepada organisasi induk. CSIRT semacam ini seper: Bank, Perusahaan Manufaktur, Universitas dll.
- **NaSonal CSIRT:** menyediakan layanan penanganan insiden kepada negara. Sebagai contoh adalah Japan CERT Coordina:on Center *(JPCERT/CC) .*
- **CoordinaSon Centers** : melakukan koordinasi penanganan insiden lintas sektor. CSIRT. Sebagai contoh adalah United States Computer Emergency Readiness Team *(US-CERT).*
- **Analysis Centers** fokus kepadan sintesa data dari berbagai macam sumber untuk menentukan tren dan pola-pola ak:vitas insiden. Contoh : *(SANS GIAC).*
- **Vendor Teams** menangani laporan tentang kerentanan di dalam produk somware dan hardware. Mereka bekerja di dalam organisasi untuk menentukan produk-produk mereka rentan atau :dak dan mengembangkan strategi mi:gasi. Vendor team juga sebagai internal CSIRT untuk organisasi tersebut.
- **Incident Response Providers** menawarkan layanan penanganan insiden dengan bentuk bisnis kepada organisasi yang memerlukannya.

Jabatan dan Pekerjaan CSIRT

- Ketua / Wakil Ketua
- Manajer atau pemimpin tim
- Asisten manajer, supervisor,
- Hot line, help desk dan star
- Incident handler
- Vulnerability handler
- Artifact analysis staf
- Platform specialist
- Trainer
- Technology watch
- Network atau System Adminitrator
- Programmer
- Staf hukum / legal

Organisasi CSIRT

- **FIRST** – Forum of Incident Response and Security
– Teams (Global/Interna:onal Ini:a:ves)
- **APCERT** – Asia Pacific Computer Emergency Response Team
– ResponseTeam(RegionalAsiaPacific)
- **OIC-CERT** – Organiza:on of Islamic Conference
– ComputerEmergencyResponseTeam
- **TF-CSIRT** – Collabora:on of Computer Security
– IncidentResponseTeaminEurope
- **ENISA** - European Network and Informa:on
– Security Agency (Regional Europe Union)
- **ANSAC** - ASEAN Network Security Action Council

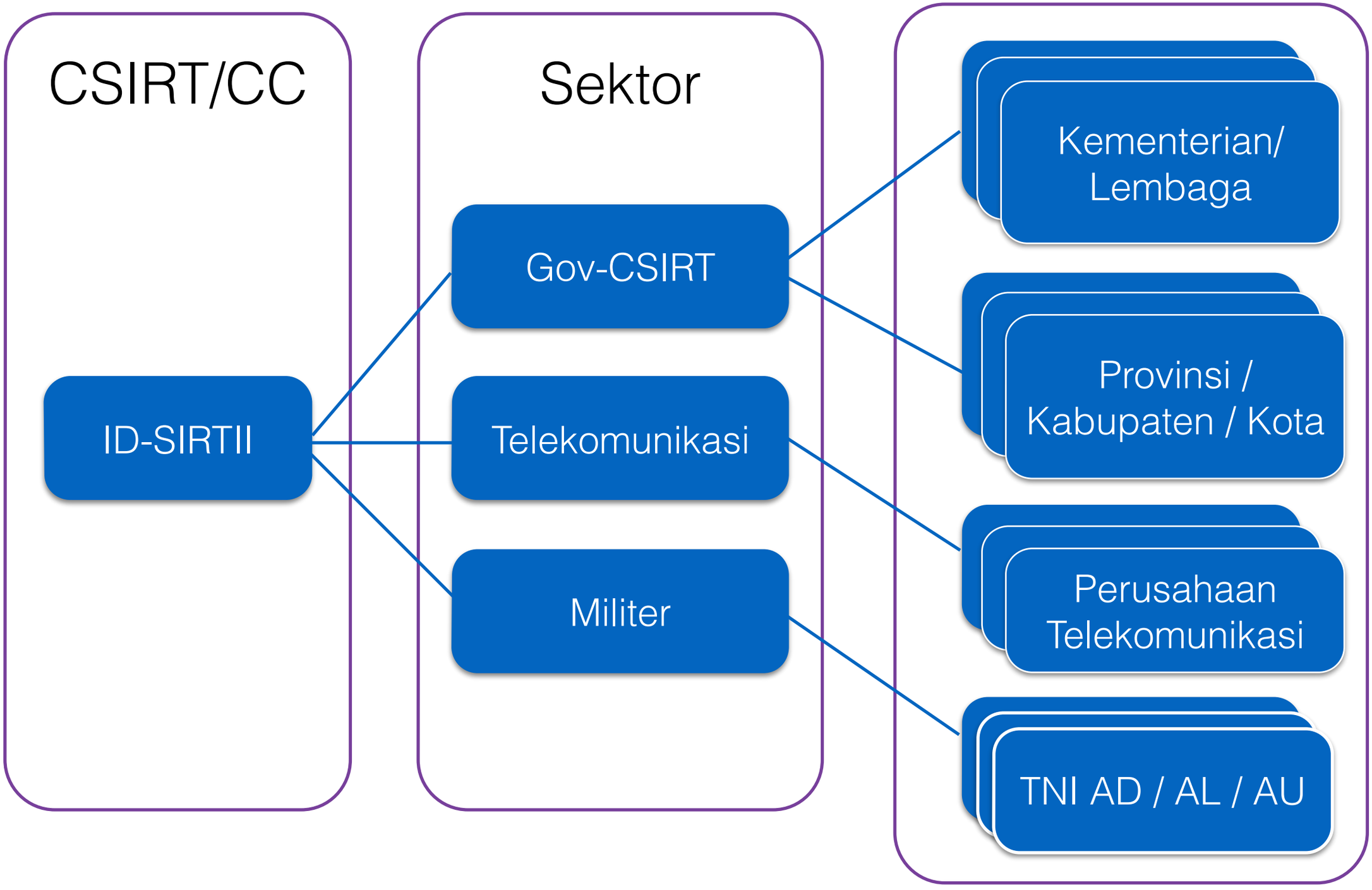
Fungsi CSIRT

- **DEFENSE** – melindungi infrastruktur kritis
- **MONITORING** – menganalisis anomaly dengan berbagai pola terdefinisi dan pola tak terdefinisi. (disebut sebagai vulnerability database).
- **INTERCEPTING** – mengumpulkan kontek spesifik atau disebut targeted content.
- **SURVEILLANCE** –mengama: dan menganalisis ak:vitas yang dicurigai dan informasi yang berubah dalam sistem.
- **MITIGATING** – mengendalikan kerusakan dan menjaga ketersediaan serta kemampuan layanan tersebut.
- **REMEDIATION** – membuat solusi untuk mencegah kegiatan yang berulang-ulang dan mempengaruhi sistem.
- **OFFENSIVE** – pencegahan/perlawanan dengan menyerang balik seperti Cyber Army dan kemampuan untuk menembus sistem keamanan.

Kemampuan CSIRT

- **PROTECT** – melakukan risk assessment, proteksi malware, pela:han dan kesadaran, operasi dan dukungan, management kerentanan dan jaminan keamanan.
- **DETECT** – pengawasan jaringan, pengukuran dan analisis keterhubungan dan situasinya, pengawasan lingkungan.
- **RESPONSE** – pelaporan insiden, analysis, response, mitigasi dan remediasi.
- **SUSTAIN** – berkolaborasi dengan MOU, kontrak pihak ketiga (vendor, provider), management (program, personnel, standar keamanan).

Struktur CSIRT Nasional



GOV-CSIRT (Government Computer Security Incident Response Team)

Pusat Monitoring dan Penanganan Insiden Keamanan Informasi Instansi Pemerintah
Kementerian Komunikasi dan Informatika Republik Indonesia

IP Reputation | Monitoring Malware Domain (IP Reputation) |

Web Links

- CERT
- CSIRT
- ID-CERT
- ID-SIRTII
- KOMINFO

Organized by :

KOMINFO

Berita | Vulnerabilty Alert

- **Facebook 'Watch naked video of friends' malware scam menginfeksi 2 juta pengguna** 11 Mar 2014
- **Malware MSIL/PSW.FakeSkype.A, Trojan Yang Suka Skype** 20 Sep 2012
- **Peluncuran Gov-CSIRT Kementerian Komunikasi dan Informatika** 20 Sep 2012
- **Win32/Spatet.A Varian Baru** 06 Sep 2012
- **10 Malware Teratas yang Mengancam Internet Indonesia** 01 Aug 2012
- **kominfo Gelar Kompetisi Jawara Cyber Untuk Rangkul Hacker Indonesia** 20 Jul 2012
- **Pengawasan Internet di US selama masa darurat** 20 Jul 2012

Call Center :
Email :
insiden@govcsirt.kominfo.go.id
Telp : 021-3845786
Fax : 021-3845786

Kegiatan Gov-CSIRT

- Memfasilitasi pembangunan CSIRT di instansi pemerintah, yg dimulai dengan mengumpulkan kontak person dari pengelola pusat data instansi pemerintah.

- Melakukan drill test (simulasi koordinasi insiden).

- Melakukan workshop penanganan webdeface, hardening server,

- Membangun Honeynet Nasional bersama komunitas Honenet Indonesian chapter.

- Membangun monitoring center menggunakan software open source.

Selesai

Kontak : riki001@kominfo.go.id