id-SIRT
Indonesia Security Incidents Response Team on Internet Infrastructure

Gunawan Hutagalung, MT
Head of Tariff and Interconnect Section
Directorate Telecommunications – DG Postel
Telecommunication Regulatory Body of Indonesia
Email: hutagalung@postel.go.id
Background

Cyber Crime Cases in Indonesia
decreasing national competitive advantage

Vulnerabilities on Critical Infrastructure
threats on national security and people’s life

Slow Adoption on Internet Usage
loss opportunities on economic growth

Absence of Strong Internet Security System
tendency of hindering internet-based activities

Challenge on Law Enforcement Practices
increasing numerous attacks on internet infrastructure

Notorious International Perception
negative image on the nation and society
Founders

MASTEL Masyarakat Telematika Indonesia
Indonesian Telematics Society

APJII Asosiasi Penyelenggara Jasa Internet Indonesia
Indonesian ISP Association

AWARI Asosiasi Warung Internet Indonesia
Indonesian Internet Cafe Association

POLRI Kepolisian Republik Indonesia
Indonesian Police Office

KEJAGUNG Kejaksaan Agung
Indonesian Attorney General Office

DITJEN POSTEL Direktorat Jenderal Pos dan Telekomunikasi
DG Postel Indonesia
Regulations

National Constitution Act UU No.36/1999
regarding National Telecommunication Industry

Government Regulation PP No.52/2000
regarding Telecommunication Practices

ICT Ministry Decree PERMEN No.26/PER/M.KOMINFO/2007
regarding Indonesian Security Incident Response Team on Internet Infrastructure

National Constitution Act UU No.11/2008
regarding Electronic Information and Transaction
The Response team

Independent Entity Representing Related Stakeholders
PROFESSIONAL - EXPERTS - POLICE - ATTORNEY - GOVERNMENT - ACADEMICIAN - RESEARCHER - PRACTITIONER

Triple Board Governance System
ADVISORY BOARD - EXECUTIVE BOARD - INSPECTION BOARD

Lead National Scale Initiatives
INTERNET SERVICE PROVIDERS AND RELATED PARTIES

Develop International Collaboration and Cooperation
INSTITUTION AND NATION BASED RESPONSE TEAMS AND OTHER RELATED BODIES
establishing CONDUCIVE and SECURE internet environment for Indonesia
The Mission

to EXPEDITE internet growth through

PROMOTING security awareness
MONITORING incident potentials
SUPPORTING law enforcement
PROVIDING technical assistance
The tasks

- EDUCATE stakeholders on security management
- MONITOR traffic, DETECT incidents, and DELIVER early warning
- GATHER, ORGANISE, STORE, and MANAGE log files
- RESPONSE to stakeholders enquiries on internet security
- DEVELOP simulation laboratories and training centres
- PROVIDE technical advisory and consultancy
- CONDUCT international collaborations and co-operations
Do not record or evaluate CONTENT implementation of and protected by INDIVIDUAL PRIVACY ACT UU No.36/1999 Article 40 on “Illegal Interception”

only monitor TRAFFIC PATTERNS and manage LOG FILES to detect threats and to support law enforcement

- Internet Traffic Behaviors
- Source, Destination, Protocol, Port, Time Stamp
The mechanism

Collect and Manage Log Files from ISPs

Monitor Internet Traffic on IXPs and NAPs

Analyse Patterns and Detect Indication Signals

Alert Related Institutions regarding Incident Occurrences

Receive Formal Requests from National Authorities

Provide Stakeholders with Log Files Record

Provide Stakeholders with Traffic Patterns Record

Develop training programs and research laboratories for societies

Engage national and international collaborations with related parties

Support stakeholders with technical information services and support
The Consequences

Operator - NAP - IXP - ISP
obligation to record logs and to monitor traffic
stated in the contract with customers

Close User Group network
obligation to record logs and users identity

Hot Spot and Internet Cafe
obligation to record users identity
The enforcement

Operator - NAP - IXP - ISP
administrative sanctions (from warning to license revocation)

Close User Group network
based on the contract agreement

Hot Spot and Internet Cafe
IP address block

lead to

CASE(s)

Legal and Law Enforcement
The topology
The tools
The organization

Ministry of ICT
Directorate of Telco & Communication

Inspection Board

Chairman

Vice Chairman

Deputy of Operation and Security

Deputy of Data Center, Applications & Database

Deputy of Education and Public Affairs

Deputy of External Collaborations

Advisory Board

General Secretary

Deputy of Research and Development

Ministry of ICT
Directorate of Telco & Communication

Chairman

Vice Chairman

Deputy of Operation and Security

Deputy of Data Center, Applications & Database

Deputy of Education and Public Affairs

Deputy of External Collaborations

Ministry of ICT
Directorate of Telco & Communication

Chairman

Vice Chairman

Deputy of Operation and Security

Deputy of Data Center, Applications & Database

Deputy of Education and Public Affairs

Deputy of External Collaborations
The holistic view

SECURE INTERNET INFRASTRUCTURE ENVIRONMENT

**MONITOR - ANALYSIS - YELL** - **DETECT - ALERT - YIELD**

- **People**
  - Advisory Board
  - Executive Board

- **Process**
  - Incident Indication Analysis
  - Incident Mngt. Support

- **Technology**
  - Traffic Monitoring System
  - Log Database System

STAKEHOLDERS COLLABORATION AND SUPPORT

NATIONAL REGULATION AND GOVERNANCE

STRONG INSTITUTIONAL RELATIONSHIPS AND COMMITMENT
The mitigation view

Discover

- Threat Intelligence
- Endpoint Intelligence
- Network Intelligence

Determine

- Correlate
- Prioritize
- Compliance

Defend

A Alert
B Block
C Correct
Thank You.

Terima kasih!