



# APCERT

*Asia Pacific Computer Emergency Response Team*

*On behalf of APCERT*

*30 August 2007*



# *About APCERT*

- **APCERT** (*Asia Pacific Computer Emergency Response Team*) is a coalition of the forum of CSIRTs (*Computer Security Incident Response Teams*).
- The organization was established to encourage and support the activity of CSIRTs in the Asia Pacific.
- Started with 15 teams / 12 economies  
→ Now 20 teams / 14 economies



# Members

## *Full Members (14):*

- **AusCERT** – *Australia*
- **BKIS** – *Vietnam*
- **CCERT** – *People's Republic of China*
- **CNCERT/CC** – *People's Republic of China*
- **HKCERT/CC** – *Hong Kong, China*
- **IDCERT** – *Indonesia*
- **JPCERT/CC** – *Japan*
- **KrCERT/CC** – *Korea*
- **MyCERT** – *Malaysia*
- **PH-CERT** – *Philippine*
- **SingCERT** – *Singapore*
- **ThaiCERT** – *Thailand*
- **TWCERT/CC** – *Chinese Taipei*
- **TWNCERT** – *Chinese Taipei*

# Members

## *General Members (6):*

- **BP DSIRT** – *Singapore*
- **BruCERT** – *Negara Brunei Darussalam*
- **CERT-In** – *India*
- **GCSIRT** – *Philippine*
- **NUSCERT** – *Singapore*
- **VNCERT** – *Vietnam (Newly joined in April 2007)*

# Objectives

- Encourage and support regional and international cooperation on information security in the Asia Pacific region;
- Jointly develop measures to deal with large-scale or regional network security incidents;
- Facilitate info sharing and technology exchange, including info security, computer virus and malicious code, among its members;
- Promote collaborative research and development on subjects of interest to its members;
- Assist other CSIRTs in the region to conduct efficient and effective computer emergency response capability;
- Provide inputs and/or recommendations to help address legal issues related to info security and emergency response across issues regional boundaries;
- Organize an annual conference to raise awareness on computer security incident responses and trends.



**Network Security  
Cooperation**



**Emergency  
Response**



**Computer Security  
Awareness**

# *How APCERT Works*

- **CSIRT: Computer Security Incident Response Team**
  - Independent from politics, market, industry
  - Do not focus on WHO (attribute) and WHY (motivation)
  - Focus on technically what is happening, how to stop the incident, how to prevent it, from technical perspective coordination
  
- **CSIRT Common Policy**
  - My security is Depending on your security
  - Web of trust – CSIRT trust relationship is developed based on a long time operation collaboration relationship
  
- **Systematic Handling – with repeatable procedure, POC agreement**
  - Time manner
  - Each team has appropriate domestic contact to handle / respond to incidents (ISPs, critical infrastructure, government...)
  - Reaching to disconnected place using CSIRT network, where it is difficult to reach

# Consistent Efforts

## Developed close collaboration relationship (Bridge the gap)

- Regular face to face meetings between teams (develop trust)
- Developing long time tactical strategy addressing cyber related issues,  
and working together
  - Training/Education/Awareness program
- Daily communication not only incident information but about team structure, problem, trend, project
- Site visiting time to time, organizing regular gatherings

## POC arrangement between members

- 24 hours hotline
- Encrypted communication tools

Incident Handling Drill

## Practice - Incident Handling Drill

- APCERT Drill 2005 (10 teams / 9 economies)
- APCERT Drill 2006 (Participation of 15 teams/ 13 economies)





## *Based on operational experience – Outreach to multiple sectors*

- One important role of APCERT is education and training to raise awareness and encourage best practice.
  - APEC-TEL: APCERT provides recommendation / situation awareness / trend to AP regional intergovernmental initiative as security experts group in AP
  - APCERT received the General Guest status at APEC-TEL
  - ASEAN: APCERT members provide CSIRT training and Outreach program to newcomer economies
  
- Cross regional collaboration
  - TF-CSIRT (TERENA's Task Force of Computer Security Incident Response Teams): European Counterpart of APCERT
  - FIRST: Implement "TRANSITS" standard CSIRT training material, add regional modules on top of the core material
    - TRANSITS program —from EU

# *APCERT Recent Activity Updates*

## *APCERT 2007 AGM, February 2007, Malaysia*

- Hosted by MyCERT

## *APEC-TEL 35 Malware Workshop, April 2007, Manila*

- AusCERT, CNCERT/CC, KRCERT/CC

## *APCERT International Incident Handling Drill 2007*

- Coming soon

## *Other International Relationships & Engagements*

- FIRST SC representative (JPCERT/CC)
- APEC Tel SPSG Deputy Convener (KrCERT/CC)