• APCERT is a coalition of CSIRTs working together under a common framework to achieve common objectives
• economies within the APNIC block and geographic boundaries of 60th degree parallel (longitude)
• started from 15 teams from 12 economies
  – Now 17 teams from 13 economies
Formation of APCERT

• Need for cross border collaboration and information sharing recognised
• Sufficient CSIRTs established within Asia Pacific
• Meeting in March 2002 in Tokyo sponsored by Japanese Government – decision to form APCERT
• Working group established to draft framework agreement
• APCERT formally established by acceptance of framework agreement in Malaysia February 2003
• Encourage and support regional and international cooperation on information security in the Asia Pacific region
• Jointly develop measures to deal with security incidents affecting APCERT economies, particularly cross border
• Facilitate information sharing and technology exchange
• Promote collaborative research and development on subjects of interest to members
• Assist CSIRTs in the region to conduct efficient and effective incident response
• Provide inputs and/or recommendations to help address legal issues related to information security and emergency response across regional boundaries
• Hold an AGM to discuss issues, priorities, work programs, build trust and hold elections
Members

Full Members (15)

- AusCERT (Australian Computer Emergency Response Team) – Australia
- BKIS (Bach Khoa Internetwork Security Center) – Vietnam
- CCERT (CERNET Computer Emergency Response Team) – People’s Republic of China
- CNCERT/CC (National Computer network Emergency Response technical Team / Coordination Center of China) – People’s Republic of China
- HKCERT/CC (Hong Kong Computer Emergency Response Team Coordination Center) – Hong Kong, China
- IDCERT (Indonesia Computer Emergency Response Team) – Indonesia
- JPCERT/CC (Japan Computer Emergency Response Team / Coordination Center) – Japan
- KrCERT (Korea Internet Security Center) – Korea
- MyCERT (Malaysian Computer Emergency Response Team) – Malaysia
- PH-CERT (Philippine Computer Emergency Response Team) – Philippine
- SecurityMap.Net CERT (Securymap Networks Computer Emergency Response Center) – Korea
- SingCERT (Singapore Computer Emergency Response Team) – Singapore
- ThaiCERT (Thai Computer Emergency Response Team) – Thailand
- TWCERT/CC (Taiwan Computer Emergency Response Team / Coordination Center) – Chinese Taipei
- TWNCERT (Taiwan National Computer Emergency Response Team) – Chinese Taipei

General Members (2)

- BruCERT (Brunei Computer Emergency Response Team) – Negara Brunei Darussalam
- GCSIRT (Government Computer Security and Incident Response Team) – Philippine
APCERT Structure

• **Steering Committee (SC)**
  – 7 teams elected by APCERT Members
  – 2 year terms
  – Determine direction and priorities of APCERT

• **Chair and Deputy Chair**
  – elected by 4/7 of SC
  – 1 year term (maximum of 4 consecutive terms)

• **Secretariat**
  – general contact point
  – Prepare minutes and reports for APCERT
  – administrative support for APCERT

• **Full Members**
  – Leading/National CSIRTs from eligible Asia-Pacific economies

• **General Members**
  – sponsored by an APCERT Member
  – no voting rights

• **Written policies and procedures**
  – APCERT agreement and mission
  – Election procedures
  – POC policy and procedures
Initiatives

• Network monitoring and early warning
• Point of Contact scheme
• Training and capacity building (Transits, APEC, ASEAN)
• Information sharing mechanisms
• Exercises
POC Scheme

• Policies and procedures to share information about serious and time critical computer threats or vulnerabilities within and between APCERT member economies
• Single POC for each economy
• Each economy determines their own POC
• POCs respond to requests for assistance from other POCs or may be provided with information for the information of that POC which may or may not be disseminated further within that POC economy
• POCs must:
  – Be contactable 24/7
  – Provide English speaking contacts
  – Have policies and procedures in place for handling incident information or disseminating threat and/or vulnerability information
POC Scheme

• POCs must:
  – Have the necessary links within its own economy to communicate with various stakeholders within their economy, eg:
    • Other CSIRTs, law enforcement, government, ISPs etc
  – Undertake to work with other POCs and APCERT members
• POCs agree to give priority to other APCERT POCs requests within its own legal, resource constraints
• POCs must agree to honour the information sharing and handling caveats imposed by the original reporting party
Questions

• What information is shared internationally vs domestically?
  – Incident data for incident resolution
  – Early warning and alerts
  – General analysis
  – Each CSIRT determines what it shares but recognised priorities
Questions

• How to build an international trust relationship?
  – Face to face meetings vital
  – Commence sharing without expectation of return
  – Provide feedback and value for contributions made
  – Establish frameworks that support information sharing
  – Government support at national and international levels
Questions

• What are the problem areas?
  – Different resource capabilities, different priorities in terms of handling incidents, legal constraints, different levels of development and capability
  – Cost of establishing and maintaining the trust relationships is vital but also expensive (ie travel)
  – CSIRTs must operate within their own economies – sometimes they don’t have the support or understanding of the various stakeholders within an economy to facilitate the CSIRT work
Questions

• How successful non-government models of international cooperation deal with trust relationships?
  – APCERT is an operation model
  – Need for APCERT was recognised and developed by the CSIRTs at the operational level
  – The governments of member economies support APCERT
  – APCERT has been successful in developing trust relationships which are now productive for its members, eg
    • effective incident response
    • Information sharing (alerts and analysis)
Beyond Asia Pacific

• APCERT is looking to link to other regional initiatives
• Education and training to raise awareness and encourage best practice.
  – APEC-TEL: APCERT engaged as a security group to provide expert advice to APEC TEL the recommendation/situation awareness/trend to AP regional intergovernmental initiative as security experts group in AP
  – 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) and European Government CERTs (EGC)
  – FIRST: Implement “Transit” standard CSIRT training material, add regional modules on top of the core material.
    • Transit program – from EU