Asia-Pacific
Economic Cooperation

APEC Project 02/2003T – Computer Emergency Response Team Awareness Raising and Capacity Building Final Report

APEC Telecommunications and Information Working Group

December 2006

APEC Project 02/2003T – Computer Emergency Response Team Awareness Raising and Capacity Building Final Report

APEC Telecommunications and Information Working Group

Published by AusCERT
December 2006

Published by
AusCERT
The University of Queensland
Brisbane QLD 4072
Australia
Tel: +61 7 3365 4417 Fax: +61 7 3365 7031
Email: auscert@auscert.org.au
Website: www.auscert.org.au

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION SECRETARIAT
35 Heng Mui Terrace, Singapore 119616
Tel: (65) 6775-6012 Fax: (65) 6775-6013
Email: info@apec.org
Website: www.apec.org

APEC Publication Number: APEC#206-TC-01.3
ISBN: 978-1-86499-874-0

CONTENTS

Executive Summary

The advent of the Internet has seen the emergence of a new type of emergency response organisation - the Computer Emergency Response Team more generally referred to as a Computer Security Incident Response Team (CSIRT). There are over 160 of these organisations as members of the Forum of Incident Response and Security Teams (FIRST) throughout the world. There are also an indeterminate number of such teams not associated with FIRST, focussed mainly on a deterministic constituency.

All of these teams exist to address a particular problem - namely the response to intruder activity in a complex environment. In their response to this problem, many nations have chosen to establish a centralised team whose sole purpose is to monitor network health and to coordinate response to attack. Such teams are required due to the complicated circumstances caused by the disparate sources of attack and number of people required in the response. This complexity means that the coordination problem is non-trivial.

The training delivered as part of this project provided a basic framework for the understanding of operational computer security, trends in Internet-based threats, logistical arrangements and the management cycle of core services. The training provided specific examples and contained practical exercises in incident handling and preparation of typical publications similar to those encountered by national CSIRTs.

Introduction

Background

With the increasing take-up of e-business and the delivery of services on line by governments, APEC economies are becoming dependent on the Internet. The protection of Internet systems in the Asia-Pacific region is critical to the region's political and economic stability and security.

Attacks on the Internet are increasing in frequency, sophistication and scale. They come in the form of viruses, worms, trojans and denial of service attacks, among others. In response to these attacks coordinating centres have been set up with the capability and expertise to advise on computer security. These organisations are called CERTs (Computer Emergency Response Team) or more generally, CSIRTs (Computer Security Incident Response Team).

The development of these capabilities that protect us from Internet based threats is directly tied to the evolution of those that perform the attacks. In this new interconnected online world, physical borders are non-existent to the would-be attacker. It is this realisation which prompts the need for a collaborative approach across all Internet-enabled economies to counter information attacks.

APEC Leaders have recognised the need for information security and the need for a collaborative approach to counter threats in both the *eAPEC Strategy* in the *Shanghai Accord* and the *APEC Leaders' Statement on Counter-terrorism*. In particular:

- Recognising the role of computer emergency response teams in addressing security incidents and exchanging information on threats, vulnerabilities, and responses; and the need to establish such teams within all APEC economies and facilitate the exchange of information among them.

- Establish institutions that exchange threat and vulnerability assessment (such as Computer Emergency Response Teams) by October 2003.

Concurrent with the initiatives on e-Security in APEC, a working coalition of CERTs and CSIRTs from the Asian economies within APNIC's geographic boundaries of 60th degree parallel (longitude) called Asia Pacific Computer Emergency Response Team (APCERT), has established guidelines to support cooperation between CERTs in the Asia Pacific region.

APECTEL 26 resolved that APEC economies not covered by the APCERT collaboration could extend their own collaboration within their respective regions and encouraged the establishment of CERTs across the whole of APEC. It further resolved that coordination between all collaborating groups would develop an APEC regional CERT capability.

It is also important that APEC Trade and Investment liberalisation is strengthened by opening multilateral trading systems, facilitating investment activities through technical assistance and cooperation, and encouraging human resource development by reducing skills discrepancies.

Purpose of Project

The APEC Secretariat's purpose in supporting this project was to facilitate higher levels of electronic security to support trade and investment by:

- raising awareness about the need for CERTs in member economies;
- developing guidelines for establishing and operating CERTs;
- providing training through three, five-day training courses. One each to be conducted in Chile; Mexico; and Peru to assist those economies to create and operate and develop CERT capacity and awareness;
- developing a communications framework to facilitate the CERT global network; and
- integrating with e-security initiatives being undertaken in other APEC economies.

Project Delivery

Project Methodology

The execution of the project was conducted with three sequential components.

Stage 1 – Preparation
Update existing AusCERT training materials to current industry acceptable standards with reference to the CERT establishment and operating guidelines.

Stage 2 – Delivery
Provide a five-day training course to each of Chile; Mexico; and Peru. These were conducted on:

Mexico:	19-23 June 2006
Chile:	4-8 September 2006
Peru:	11-15 September 2006

Stage 3 – Reporting
A report on the project outcomes is sent to the oversight committee and the TEL.

Provision of Training

The five-day training course was developed and delivered for technical staff new to the field of computer security incident handling, and the management staff charged with overseeing a CSIRT.

In each country of Chile; Mexico; and Peru, participants were sought out in advance from a mixture of relevant government departments, private organisations and academic institutions. This has proven to be successful in previous training courses, and was seen to be useful by the participants in all three instances of training during this project. Participants were given several opportunities during the courses for both presenter-led and participant-initiated group discussions, allowing for dialog and relationship building between sometimes quite diverse organisations.

The aim of the training course was, upon successful completion, to provide participants with the following knowledge and abilities:

- Understand the incident handling life cycle
- Demonstrate basic skills in incident handling and vulnerability assessment
- Define and work to policies and procedures, and identify pitfalls
- Understand the infrastructure required to operate a successful CSIRT
- Understand the environment which the individual and the team must operate in
- Demonstrate an understanding of important computer security concepts
- Discuss the history of the Internet and important security events

While the attachment, “Training Course Module List”, provides a breakdown of the mandatory topics covered as part of each course, additional ad-hoc presentations and discussions were conducted throughout the course as they were raised by participants and with time permitting. This included a more detailed history of Internet-based identity theft with the use of case studies and the review of a high profile hacking case involving an Australian Internet provider.

Survey Findings

Participants were encouraged to complete a standard anonymous workshop evaluation form to assess the following points:

- Was the presentation material clear and easy to understand?
- What was the priority of each module in relation to the individual?
- What was the level of content quality for each module?
- Did the training course cover all the information expected, and if not, what additional topics do you believe should have been discussed?
- Were the presenters easily understood and explained concepts to your satisfaction?

The results of the survey from each country illustrated a consistently high level of quality for the course content and the delivery by the presenters. As is to be expected, the priority level varied between individuals for each module, likely influenced by the participant's job function and prior learning.

The open ended question relating to whether the training course covering the information expected by participants received several positive responses reaffirming an appropriate depth and breadth for the overall course content. Suggestions for additional content were largely grouped into the following categories:

- Provide additional examples and techniques for technical investigation
- Provide a list and description of other types of software and tools available
- Provide hands-on exercises in a computer lab environment

While these are valid and useful suggestions, items such as providing additional examples and hands-on exercises are typically not practical in the limited time allotted for the adequate explanation of the core topics in the training course and are beyond the scope defined for this project. One recommendation for addressing these requests is the provision of a separate and more technically focused training course designed for the staff directly involved with the investigation and handling of computer security incidents.

Attachment

Training Course Module List

Workshop Introduction
- Introduction of Presenters and Participants
- Overview of Course Structure

History of CSIRTs
- What is a CSIRT
- CSIRT History
- AusCERT Overview
- FIRST
- APCERT

Security Incident Trends
- Incident Trends
- Common Attacks
- Intruders
- Results of 2006 Australian Computer Crime and Security Survey

CSIRT Pre-Establishment
- Mandate and Mission
- Constituency and Contact Network
- Finance
- Legal
- Services and Scope
- Staff and Resources

Infrastructure
- Equipment
- Network Security
  - Access Requirements
  - Network Services
  - Firewalls
  - Security Domains
  - Design
- Security Administration Tools

Information Architectures
- Contact Database
- Incident Database
- Incident Deports
- Finding Contacts for Incidents
- Incident Handling Tools

Incident Handling Life Cycle
- Handling Incidents
- Definition of an Incident
- Phase 1 - Preparation
- Phase 2 - Identification
- Phase 3 - Containment
- Phase 4 - Eradication
- Phase 5 - Recovery
- Phase 6 - Follow-up
- Example Security Incident

Incident Types and Examples
- General Incident Categories
- Directly reported and immediate attention
- Indirectly reported
- Potential problems but not yet high impact

Incident Handling Examples
- Scans/Probes
- Denial of Service
- Distributed Denial of Service
- System Compromise
- Application Compromise
- Virus/Worms
- ID Theft
- Spam, Fraud, and Hoaxes
- Queries
- Vulnerabilities and Advisories
- Media
- Police
- Government
- CSIRT Teams
- Crazy People
- Physical Attack / Disaster Recovery
- Threats
- DNS or Proxy Poisoning
- Accidents
- Mailing List Requests
- Wrong Time Zone
- Copyright Infringement

Incident Investigation Techniques

- Finding Incident Contacts
- Internet Registries
- Autonomous Systems
- Fraudulent Domains
- Malware Analysis
- Google

CSIRT Procedures

- Policies, Procedures, Standards, Guidelines
- Evolution of Procedures
- Benefits of Procedures
- Example of Policy-Procedure Life Cycle
- CSIRT Procedures Manual
- Class Exercise

Day to Day Activities

- Keeping Up-to-Date
- Answering the Phone
- Visitors
- Point Duties
- Backup Point Duties
- General System Administration
- Meetings
- On-Call

CSIRT Publications

- Publication Types and General Rules
- Advisory Life Cycle
- Example
- Class Exercise

CSIRT Management Issues

- Operations
- Staff
- Metrics
- Finance
- Reporting

Workshop Conclusion

- Review of Salient Topics from Previous Modules
- Where To Go From Here

Note: Incident handling group exercises are conducted throughout the course, in addition to any module-specific class exercises that are listed above.

Published by
AusCERT
The University of Queensland
Brisbane QLD 4072
Australia
Tel: +61 7 3365 4417 Fax: +61 7 3365 7031
Email: auscert@auscert.org.au
Website: www.auscert.org.au

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION SECRETARIAT
35 Heng Mui Terrace, Singapore 119616
Tel: (65) 6775-6012 Fax: (65) 6775-6013
Email: info@apec.org
Website: www.apec.org

APEC Publication Number: APEC#206-TC-01.3
ISBN: 978-1-86499-874-0