Organizational internal computer security incident responding structure: CSIRT

JPCERT Coordination Center, Japan
Manager of Watch and Warning Group
Keisuke Kamata
Agenda

- Concept of Incident response.
  - What is computer security Incident?
  - Necessity of organizational incident response
  - What is CSIRT?

- How to create a CSIRT?
  - From JPCERT/CC experience
Message of this presentation

- We must **recognize** the importance of considering information security issues within an organization.

- To considering information security issues, one of the important point is having a capability to **respond computer security incidents** as a technical standpoint.

- **CSIRT**: Computer Security Incident Response Team is a good model to handle computer security incident.

- Make an organizational internal **CSIRT** within your organization.
Concept of Incident Response

Incident = Computer Security Incident
What is computer security incident?

In order to respond we must recognize “computer security incident” at first

- No uniform agreement as to what constitutes an incident
- No same definition for different organization
- It’s depend on what the organization wants to
- Incident is a things which should be handled
What is the “Incident Response”?  

- “Incident Response” is the process of addressing computer security incident.  
  - Detecting / Analyzing the incident  
  - Limiting the incident effect

- General goals are:  
  - The progress of the incident is halted.  
  - Affected systems return to normal operation.
Why Do I Need a Incident Response?

- Malicious acts will happen
  - Even the best information security infrastructure can NOT guarantee.
  - Attacker wants to do malicious activities
    - What is their motivation?
      - Technical interests → Money

- If Incidents occur, it is critical to have an effective means of responding.

- To limit the damage and lower the cost of recovery
  - Need to have the ability: Protect, Detect, Analyze and Respond to an incident.
  - Professional should respond to an Incident
Incident Response overview

- Gather and Share Information
- Planning for Response
- Planning for Detection
- Formulation of organizational structure

Prepare

Detect

Response

- Actual Response planning
- Actual Response
- Coordinate between stakeholders
- Closing and Recording incident

- Incident Reporting Framework
- Monitoring system (server and network)
- Triage, Prioritize
To implement the organizational framework for incident response

— Identify the currently performance of incident response in an organization
  - Detecting, Triaging, Responding the computer security incident

— Link and combine them
  - Assign Roles and Responsibilities, Identify the appropriate Point of Contact, Design the Communication Flow

— Be in a consistent and systematic manner

*Develop the Organizational Response for Computer Security Incident*
Information sharing and cooperation within an organization
  — Unification of Incident reporting or security events gathering points
  — Implementation of Interorganizational communication and setting the coordinating point

Relationship to external security team
  — To request the support to resolve the incident which is of external origin, such as DDoS or Phishing.
  — Unification of receiving the security events and incidents from outside.
  — Build a web of trust in order to work with other teams

Will tell more detail in other slides.
It is important to formulate incident response plan before occurring the incident

Key points for formulating the organizational response plan

— Comprehension of the complex computer network and system
— Clarification of the person in charge of incident response and the responsibility of incident responder
— Unification of Incident Reporting
— Implementation of technical supporting for the on-site incident response activities, providing the know-how for incident response and related information
— Constructing the policy and procedure for incident response activities.
— (If requesting of support to external organization,) taking hold on what the external organizations are able to do, and how to request
Internal CSIRT

— CSIRT: Computer Security Incident Response Team
— A Team which take charge of incident response in an organization
— Depending the organization, a response capability as a CSIRT is implemented by doubling CSIRT manager/staff as other work assignment

Best Practice model for Organizational Response Structure = Internal CSIRT
If planning and conduct the incident response after occurring, it expanding the damage. So, it is needed to build CSIRT before occurrence of the incident.
Functions of Internal CSIRT

**Inside functions**
- Provide the single point of contact for incident reporting for constituency in an organization
- Support for on-site incident response, or providing technical know-how and related information
- Support for organizational decision-making during incident responding
- Coordinate the interorganizational communication on incident information
- Improve the business system user’s awareness of information security

**Outside functions**
- Coordinate with external security teams
- Keep up on the latest move in the information security
- Gathering the latest information related to computer/network security, and share with the constituency/other teams that need to know
Advantage of setting Internal CSIRT is depending from size and business type of an organization

Major benefits are as follows:

—Managing the information relevant to incident

—Providing a central point of contact

—Establishing the trusted relationship needed for respond

* The following 3 slides show the details.
Advantage of Setting CSIRT (2)

Managing the information relevant to incident

1) Realization of centralized security information management and sharing
2) Streamlined decision-making of incident response
Advantage of Setting CSIRT (3)

- Providing a central point of contact

1) Getting the trusted broker by communicating the direct incident information
2) Realization of consolidate information from the outside
Advantage of Setting CSIRT (4)

- Establishing the trusted relationship needed for response

1) Increasing the information content needed for incident response
2) Ready to address to any situation
Recommend setting CSIRT

- **Setting Internal CSIRT is strongly recommended!**
  - As best practice model of organizational incident structure, that taking charge of limiting the extent of damage and recovery from incident
  - As effective measure to collaborate/coordinate with the external security teams

- **CSIRT Community**
  - Spreading around the world with creating the community and conducting the training
    - FIRST (Forum of Incident Response and Security Team)
    - APCERT (Asia Pacific Computer Emergency Response Team)
      - [http://www.apcert.org/](http://www.apcert.org/)
    - TF-CSIRT (Task force that promoted collaboration between CSIRTs at the European)
Incident handling by the internal CSIRT

- Proper incident handling in predefined constituencies
- For example
  - Point of Contact
  - Triage
  - Prioritization the problems
  - Technical assistance
  - Solution, suppression of damage, assistance to recovery
How to create a CSIRT?
The definition of incidents differ from organization to organization and are based on

- enterprise contents, enterprise scales, department structure
- how the business is handled, the threat toward the business and the risk.

- JPCERT/CC definition

  - Human manipulation related to computer security
  - Abuse of resources, denial of service, breaking data information leakage

- Events that related to system or network securities
- Security policy breach/contravention
Framework of internal CSIRT activities

Define the following fundamentals to establish the framework of internal CSIRT activities

1. **Mission statement**
   - Objectives, goals – what to achieve

2. **Constituency**
   - Who to target
   - Relationship with the constituency
   - Reconcilability by the constituency
   - Trust relationship with the constituency

3. **Position in the organization**
   - Position of CSIRT
   - Role of CSIRT
   - Mutual relationship with relating departments

4. **Relation with other teams**
   - Cooperation and collaboration with other CSIRTs
Clarify the role expected by the organization

Create the mission statement that will supplement the organization’s objectives

Obtain understanding from the management layer of the organization that the internal CSIRT belongs to

The "mission statement" should be announced widely to the constituency as well as other CSIRT teams in order to obtain understanding of role, objectives and activities of internal CSIRT
Define the area of internal CSIRT activities
  - In other words, “define the target services”

Setting the authority that the internal CSIRT possesses to the constituency
  - Authority over constituency?

Announce the services of internal CSIRT to the constituency
  - Awareness as the incident reporting POC

Earn trust from the constituency
  - No trust, no incident reports
Clarify the expected role of internal CSIRT in terms of the overall risk management
- Mainly managing the risks caused by information security infrastructure

In case there is already an existing incident response team, clarify/distinguish each mission statement and constituency

Clarify the responsibility of internal CSIRT in the organization
Clarify the coordination role of the internal CSIRT with other external CSIRTs

Understand the capacity, function and role of other CSIRTs
  - It is also important to notify what the internal CSIRT can do to other CSIRTs

Define what is necessary to cooperate with other CSIRTs
  - It is necessary to establish trust-relationship with other CSIRTs to gain cooperation due to the nature that most incident handling requests are self-initiative and unofficial.
### CSIRT Services example

#### Reactive Services
- **Alerts and Warnings**
- **Incident Handling**
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- **Vulnerability Handling**
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- **Artifact Handling**
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

#### Proactive Services
- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

#### Security Quality Management Services
- Risk Analysis
- Business Continuity & Disaster Recovery Planning
- Security Consulting
- Awareness Building
- Education/Training
- Product Evaluation or Certification
Key Points of internal CSIRT activities 1

- The desired role/function
  
  Proper handling, assistance of recovery to the incidents that happened within the organization

- Prospects 1
  
  Define the “incident” for the organization
  
  - Analysis of the past incidents
  - Understand the incidents in other companies in the same trade
  - Recognize/analyze incidents among Management layer and field employee
  - Recognize/analyze incidents that possibly will happen
  - Incidents categorization

Basic policy of Internal CSIRT will be decided by defining the “incident”
Prospects 2

- Method of appropriate correspondence/response, and define the advance preparation
  - Check the integrity of incident reports before start the incident handling
    - Publicize the POC to the constituency as best in advance
  - Discussion what can do/ cannot do considering the 「constituency」 and 「position in organization」
  - Understand/discuss of what the internal CSIRT can do/cannot do
    - For the condition that need assistance of external organization, consider the collaboration in advance
  - Understand/consider the appropriate response expected by the administration layer and constituency

Acquiring the lists of 「appropriate response」 and what to do prepare in advance
Conclusion

- Know about “computer security incidents”

- Think about Incident Response

- Think about Organizational Incident Response

- Prepare for computer security incidents
  - Organizational internal CSIRT is a good model
  - ThaiCERT will help you, and JPCERT/CC help ThaiCERT 😊

- Communication is a “key” for effective incident response
  - Within your organization
  - Between organizations
Public CSIRT Materials

CERT/CC: CSIRT Development

http://www.cert.org/csirts/

ENISA: A step-by-step approach on how to setup a CSIRT


AusCERT: Forming an Incident Response Team


RFC2350: Expectations for Computer Security Incident Response

http://www.ietf.org/rfc/rfc2350.txt
Thank you for your attention.

■ JPCERT Coordination Center
  - office@jpcert.or.jp
  - Tel: +81-3-3518-4600
  - http://www.jpcert.or.jp
  - Vulnerability Information : http://jvn.jp

■ Incident Report
  - info@jpcert.or.jp
  - PGP Fingerprint:
    BA F4 D9 FA B8 FB F0 73  57 EE 3C 2B 13 F0 48 B8