Security Incident Response Contact Repository Implementation

Luis Diego Espinoza (Chair)
Antoinette Johnson, .vi
Isak Jacobsen, .fo
Hitoshi Saito, .jp
Mohamed Ibrahim, .so
Wim Degezelle, CENTR (observer)

http://ccnso.icann.org/workinggroups/iriwg.htm
Computer Incident Response Team

Figure 3: Service and Quality Framework as Derived from Mission Statement

### Table 4: List of Common CSIRT Services

<table>
<thead>
<tr>
<th>Reactive Services</th>
<th>Proactive Services</th>
<th>Security Quality Management Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Alerts and Warnings</td>
<td>- Announcements</td>
<td>✓ Risk Analysis</td>
</tr>
<tr>
<td>+ Incident Handling</td>
<td>- Technology Watch</td>
<td>✓ Business Continuity &amp; Disaster Recovery Planning</td>
</tr>
<tr>
<td>- Incident analysis</td>
<td>- Security Audit or Assessments</td>
<td>✓ Security Consulting</td>
</tr>
<tr>
<td>- Incident response on site</td>
<td>- Configuration &amp; Maintenance of Security Tools, ...)</td>
<td>✓ Awareness Building</td>
</tr>
<tr>
<td>- Incident response support</td>
<td>- Development of Security Tools</td>
<td>✓ Education/Training</td>
</tr>
<tr>
<td>- Incident response coordination</td>
<td>- Intrusion Detection Services</td>
<td>✓ Product Evaluation or Certification</td>
</tr>
<tr>
<td>+ Vulnerability Handling</td>
<td>- Security-Related Information Dissemination</td>
<td></td>
</tr>
<tr>
<td>- Vulnerability analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Vulnerability response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Vulnerability response coordination</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+ Artifact Handling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Artifact analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Artifact response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Artifact response coordination</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Contact Repository within CSIRT

Incident Handling Service

- Announcement Function
- Triage Function
- Information Handling

Service Description
Service Functions Overview
Feedback Function
Interactions
Points of Contact
Contact Repository
ccTLD Point of Contacts for Incident Response Services

- Contact Repository Implementation Working Group
- Explore factors to implement, maintain and operate the repository.
- Funding models
- Governance models
Repository Operation

- Database: Directory Service System
- Maintain and Operate: Contact Management Services
Relationship of Major Components

- Standing Committee
- Incident Response Entities (CERTs and others)
- Subscribers
- ccTLD registries
- Contact Service Center
- Directory Services
- Contact Repository

Legends:
- red angled line: Processes of Query/Browse
- blue curved line: Processes of Update
- purple dotted line: Processes of User Management
- brown line: Processes of Governance
- green line: Processes of Incident Handling
Directory Service System

- **Browsing**: SearchContacts
- **Processing**: CreateContact, UpdateContact, DeleteContact

TCF: tools
- WUI, LDAP, E-MAIL
Maintain and Operate
Keep contacts updated

- 24/7/365 Operation
- E-mail response management
- Web Chat
- Session recording and transcript mailing
- Self-service Knowledge-base
- Analytics and Quality System
- Telephony infrastructure
- Interactive Voice Response (IVR) technology
### Frequency and rotation of communication methods

- Complete update every 3 months.

<table>
<thead>
<tr>
<th>Estimated Monthly outbound contacts volume</th>
<th>Number of TLDs</th>
<th>Number of contacts in the repository</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>200</td>
<td>400</td>
</tr>
<tr>
<td></td>
<td>1000</td>
<td>2000</td>
</tr>
<tr>
<td></td>
<td>5000</td>
<td>10000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Criteria of frequency</th>
<th>1/15 monthly</th>
<th>Voice</th>
<th>Email</th>
<th>Fax</th>
<th>Chat</th>
<th>Letter/telegram</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>13</td>
<td>67</td>
<td>67</td>
<td>13</td>
<td>67</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>333</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>67</td>
<td>67</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>333</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>67</td>
<td>67</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>333</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>67</td>
<td>67</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>333</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Proposed Standing Committee to govern the repository

- ccNSO establishes Standing Committee
- Standing Committee reports to ccNSO Council and users.
- Standing Committee is supported by ccNSO Secretariat and with experts assistant from SSR department.
- Manage Service provider (Agreement compliance)
- Relation with subscribers.
- Maintain use cases of the repository.
Proposed Funding Models

- Uniform subscription and set-up fee.
- Cross-ccTLD funding
- ICANN funding (using part of the financial contribution).
- Mixed funding (additional support by more affluent ccTLDs combined with ICANN funding)
Next steps

- Send the Request of Information (ROI) to potential providers
  - To adjust specifications and ideas of possible costs.
- With the feedback of ROI, convert the document in a Request for Proposal for the ccNSO Council.
- Sent the Request For Proposal (RFP), approved by the ccNSO Council to potential bidders.
- Analyze and recommend the best offer to the ccNSO Council.
Questions?