Incident Response WG – Status

Joerg Schweiger
WG Chair <ccnso-erpwg@icann.org>
<schweiger@denic.de>
Cartagena, December 2010, ICANN ccNSO Meeting
Purpose

- assist in implementing sustainable mechanisms for the engagement of and interaction with ccTLD registries during incidents that may impact the DNS

Scope

- repository of ccTLD contacts and channels of communication for incident response
### Work plan

<table>
<thead>
<tr>
<th></th>
<th>Define what is considered to be an <strong>incident</strong></th>
<th>March, 10th</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Define the <strong>use cases</strong> of the contact repository for ccTLDs</td>
<td>April, 30th</td>
</tr>
<tr>
<td>3</td>
<td>Define <strong>escalation procedures</strong> and <strong>action paths</strong></td>
<td>May, 30th</td>
</tr>
<tr>
<td>4</td>
<td>Define the repository <strong>data model</strong> to accomplish the use cases</td>
<td>Brussels meeting (June)</td>
</tr>
</tbody>
</table>
| 5 | (Towards the ) **Implementation of** the contact repository  
   • Make or Buy?  
   • Suggestions to who will **run and maintain** the repository at what level of acceptable **expenditure** covered by whom | Cartagena |
| + | See to the discussions refering to the DNS-CERT initiative | since Nairobi |
Make or Buy?

Buy

- **Trusted Introducer**
  - meets / could easily be adapted to the contact repository’s data model and use case requirements
    - browse through a list of alphabetically listed contacts
      - data is kept up-to-date by the operator
    - „secured“ email communication
    - „Internet-based“ communication and voice mail and SMS
  - redundantly operated in 2 data centers
  - per participant: 1,400 $ p.a. + (one time) set up fee: 1,300 $
  - used by CSIRTs

- **Packet Clearing House tool**

Make

- „browse“ or „query“ solution (resulting in different look & feel and maintenance models)
Make or Buy?

Functional and non-functional „must-have“ requirements

- Support the envisioned use cases
- High availability 24/7
- Alternative communication channels (not using the internet)
- Data is kept up-to-date

¿ Anything else?
Further steps can’t be done nor decided by the WG (alone) …

- Make or buy decision and sophistication level of the contact repository implementation heavily depends on financing abilities
  - Completely covered by ICANN
  - ICANN covers implementation, each participants pays for operational cost
  - Cost per participant is completely covered by the respective participant
  - Sponsoring models
  - Fixed pricing no matter how many participants
  - ...

Further steps can’t be done nor decided by the WG (alone) …

Decisions?!

1. The ccNSO council / ICANN to suggest and seek input from the community on financing
2. The ccNSO council / ICANN to task further examination, selection and implementation given the framework of data model, use cases and must-have requirements
3. Close down the IR WG
Backup

Joerg Schweiger
ccnso-erpwg@icann.org
schweiger@denic.de
+49 69 27235 -455
Incident

Large scale, unintended misfunction of the DNS or systematic, rigorous preparation of or actual attack on

- the availability of the DNS or registration systems
- the data integrity or privacy of the DNS or registration systems
- the stability or security of the internet at large

where a coordinated international response by operators and supporting organisations is advised.

Not considered to be an incident for the purpose of this WG is

- the malicious use of the internet itself (e.g. SPAM, …) or
- the unlawful use or misuse of specific domains / content (child pornography, …)
- any routing problems (BGP, …)
Use cases

• **Information exchange**
  - Provide a security contact point under any circumstances
  - Issue early warnings

• **Counter action**
  - Inform the “participating community” about “an incident”
  - Facilitate/enable community support for “a community member”

Dismissed … at least for a first version of the repository and its usage

• Generate reports on prevention best practices (technical, process related)
• Store/compile/give access to mitigation lessons learned
• Provide generic action plans ➔ reflect this in the charter
• Coordinate responses
<table>
<thead>
<tr>
<th>Work plan action item 3: Contact repository data attributes</th>
</tr>
</thead>
</table>

- Internet domain
- ccTLD operator name
- Host organization of ccTLD response contact point
- Registry operator name

<table>
<thead>
<tr>
<th>Name of person representing the team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function/role of the person</td>
</tr>
<tr>
<td>Authentication information of the person, incl. encryption keys</td>
</tr>
<tr>
<td>Country the contact is located</td>
</tr>
<tr>
<td>Time zone of the contact</td>
</tr>
<tr>
<td>Business hours (relative to UTC)</td>
</tr>
<tr>
<td>Regular telephone number (country code, telephone number)</td>
</tr>
<tr>
<td>Emergency telephone number (country code, telephone number)</td>
</tr>
<tr>
<td>(specific) Email address</td>
</tr>
<tr>
<td>Messenger services (service, id)</td>
</tr>
<tr>
<td>Facsimile number (country code, fax number)</td>
</tr>
<tr>
<td>Other telecommunication facilities</td>
</tr>
<tr>
<td>Language</td>
</tr>
</tbody>
</table>

- Name of substitute person representing the team
Questions?

Joerg Schweiger
ccnso-erpwg@icann.org
schweiger@denic.de
+49 69 27235 -455