Incident Response WG – What’s next?

Joerg Schweiger
WG Chair
<br>
<schweiger@denic.de>
<br>
Singapore, June 2011, ICANN ccNSO Meeting
Charter

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
Use Cases for the Contact Repository

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

⇒ Work plan
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
### Contact repository data attributes

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

| Name of substitute person representing the team |

---
How to move on? (1)

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  ➔  Set-up the Implementation WG
Questions?

Joerg Schweiger
schweiger@denic.de
+49 69 27235 -455
Backup

Joerg Schweiger
ccnso-erpwg@icann.org
schweiger@denic.de
+49 69 27235 -455
Work plan action item 1: Definition Incident

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, …)