Incident Response WG – current status

Joerg Schweiger
WG Chair <conso-erpwg@icann.org>
<schweiger@denic.de>

Nairobi 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
• qualification of
  • incidents
  • escalation procedures
  • action paths
## Work plan

<table>
<thead>
<tr>
<th></th>
<th>Define what is considered to be an <strong>incident</strong></th>
<th>March, 10 th</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Define the <strong>use cases</strong> of the contact repository for ccTLDs</td>
<td>April, 30 th</td>
</tr>
<tr>
<td>3.</td>
<td>Define <strong>escalation procedures</strong> and <strong>action paths</strong></td>
<td>May, 30 th</td>
</tr>
<tr>
<td>4.</td>
<td>Define the repository <strong>data model</strong> to accomplish the use cases</td>
<td>Brussels meeting</td>
</tr>
<tr>
<td>5.</td>
<td>Suggestions to <strong>who will implement, run and maintain the repository</strong> at what level of acceptable <strong>expenditure</strong> covered by whom</td>
<td>Brussels + 1 month</td>
</tr>
</tbody>
</table>
**Definition: Incident** (to be revised frequently)

Systematic, rigorous preparation of or actual attack on

- the availability of the DNS or registration systems
  - DDOS, EPP flaw exploit
- the data integrity or privacy of the DNS or registration systems
  - Zone enumeration, cache poisoning, social engineering
  - was: conficker; will be: ???
- the stability or security of the internet at large

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

Considered not 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, ...)
Current discussions

1. Contact repository - Sophistication requirements?
   - Who is entitled to access?
   - Needed security level of access and communication means?
   - Hosted by a professional third party or dedicated ICANN branch or just an IANA database extension?

2. Escalation procedures and action paths
   - Definable in a useful way or “just generic”?

3. Relation / Delineation with respect to existing organisations obliged with related or similar tasks
   - DNS-CERT, DNS-OARC, SSAC, RSIG, CERTs/CSIRTs, FIRST, BTF, ISC SIE, gTLD-initiative?
Questions?

Joerg Schweiger
ccnso-erpwg@icann.org
schweiger@denic.de
+49 69 27235 -455
Contact repository data attributes (first draft)

- ccTLD name
- Name of person representing the team
- Host organization of ccTLD response contact point
- Country the contact is located
- Internet domain
- Regular telephone number (country code, telephone number, time-zone relative to UTC):
- Emergency telephone number (country code, telephone number, time-zone relative to UTC):
- Email address
- Messenger services (service, id)
- Facsimile number (country code, fax number)
- Other telecommunication facilities
- Language
Use cases (first draft)

- **Information exchange**
  - Provide a security contact point under any circumstances
  - Generate reports on prevention best practices (technical, process related)
  - Store/compile/give access to mitigation lessons learned

- **Proactive actions**
  - Provide generic action plans
    - Generate reports on potential threats

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