Incident Response WG – current status

Joerg Schweiger

WG Chair <ccnso-erpwg@icann.org>

<schweiger@denic.de>

Brussel, June 2010, 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
- qualification of
  - incidents
  - escalation procedures
  - action paths

Work plan

✓	1.	Define what is considered to be an incident	March, 10 th
✓	2.	Define the use cases of the contact repository for ccTLDs	April, 30 th
✓	3.	Define **escalation procedures** and **action paths**	May, 30 th
✓	4.	Define the repository data model to accomplish the use cases	Brussels meeting
	5.	Suggestions to **who will implement, run and maintain the repository** at what level of acceptable **expenditure** covered by whom	Brussels + 1 month

➔ Next steps

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, …)

➔Work plan

Work plan action item 2: 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 migitation lessons learned
- Provide generic action plans ➔ reflect this in the charter
- Coordinate responses

➔Work plan

Work plan action item 3: Contact repository data attributes

<table>
<tr><td colspan="2">• Internet domain
• ccTLD operator name
• Host organization of ccTLD response contact point
• Registry operator name</td></tr>
<tr><td>• Name of person representing the team
• Function/role of the person
• Authentification information of the person, incl. encryption keys
• Country the contact is located
• Time zone of the contact
• Business hours (relative to UTC)
• Regular telephone number (country code, telephone number)
• Emergency telephone number (country code, telephone number)
• (specific) Email address
• Messenger services (service, id)
• Facsimile number (country code, fax number)
• Other telecommunication facilities
• Language</td><td>• Name of substitute person representing the team</td></tr>
</table>

➔Work plan

Further discussions / decisions to be made

1. Contact repository - Sophistication requirements ?
   - Who is entitled to access? ➔ accessible by *TLDs*, DNS operators and registry operators
   - Tools / means / functionality? ➔ mailing list
   - Needed security level of access and communication means?

2. 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, Conficker WG?

Charter update concerning DNS-CERT

Updated /amended part of the charter …

„… the working group will

- include aspects of and relations with ICANN’s DNS-CERT initiative it considers to be relevant and appropriate, if any.
- seek input and feed-back from the ccTLD community and coordinate the input and feed-back from the ccTLD community on the DNS-CERT initiative “

- Comments (by the ccNSO council and others) towards the ICANN DNS-CERT initiative were submitted, but yet haven’t been addressed sufficiently.
  At this point, **no further commenting is necessary**, unless ICANN proposes a different or adopted approach.
- If ICANN will initiate steps towards the called for bottom-up multi-stakeholder approach to further ensure DNS security and stability the IR WG will gather the ccNSO’s members input to comment on those or **actively participate to jointly set up an appropriate approach** or collaborate with the joint WG of the NSOs

Questions?

?

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