Incident Response Working Group Call

9 October 2009

Attendees:

Bart Boswinkel, ICANN
Wim Degezelle, CENTR (observer)
Stephen Deerhake, .as
Luis Espinoza, .cr
Eric iriarte, LACTLD
Yurie Ito, ICANN
Otmar Lendl, .at
Janantha Marasinghe, .lk
Orange Morishita, .jp
Kristina Nordström, ICANN
Norm Ritchie, .ca
Hugo Salgado, .cl
Katrina Sataki, .lv
Eswari Sharma, .np
Save Vocea, ICANN

Apologies:

Ondrej Filip, .cz
Ben Fuller, .na
Nigel Roberts, .gg

Agenda

1. Election of chair

- Norm Ritchie welcomed everybody to the call and acknowledged the extensive interest for participation in the Incident Response Working Group (IR WG)

- *Bart Boswinkel* suggested that a chair from the ccTLD community should be appointed. *Stephen Deerhake* nominated Norm Ritchie to be the chair and Eric Iriarte seconded the nomination. Norm Ritchie accepted and was formally appointed as Chair of the Working Group (from here on also referred to as the Chair). It was decided that a co-chair will be selected on the WG email list.

Action 01-01:
The Incident Response Working Group members to select and appoint a co-chair for the Working Group on the email list.

2. Inclusion of technical experts in the WG as observers.

- The Chair noted that several non-ccTLD related technical experts are interested in participating in the IR WG. The Chair asked the members if there were any comments or objections to the participation of people from these two groups. *Bart Boswinkel* suggested that volunteers from these groups should be sent formal invitations from the Working Group Chair, to avoid making the Working Group public for anyone to join.

- For avoidance of doubt it was established that ccTLD related participants are all full Working Group members. As is the case for other ccNSO Working Groups, ther is no disctinction between ccTLD who are members and non-mebers of the ccNSO. The technical experts are invited as observers.

Action 01-02:
The Chair to invite technical experts to the Incident Response Working Group.

3. Proposed working method

- *Bart Boswinkel* explained that the basic idea of the working method is to present relevant documents using the email list, gather comments from Working Group members and then based on the comments modify the document and follow up with discussions leading up to finalisation of the document.

- The comment period for the Draft Plan was set to end on 13 October. The second draft is to be published on 16 October.

Action 01-03:
Incident Response Working Group members to provide input and feedback before 13 October.

Action 01-04:
NormRitchie and Yurie Ito to update the second Draft Plan and prepare it for publication.

Action 01-05:
The ccNSO Secretariat to publish the updated Draft Plan for comments.

4. Clarification draft plan

- The Chair noted that this topic was covered in the previous agenda item.

5. Comments and input on draft plan

- The Chair referred to a comment on the Draft Plan saying that the Working Group should be not only reactive but also proactive and agreed to the statement, as did the rest of the Working Group. The Chair pointed out that in

order to be a proactive group it needs to prioritise the development of contact lists.

- *Bart* suggested that for the updated Draft Plan there should be a clarification about the priorities of the IR WG. The Chair agreed.

Action 01-07:
Yurie Ito and Norm Ritchie to identify priorities in draft, based on input and feedback of Working Group members.

- The Chair suggested that to improve the documents for the Working Group it could be a good idea to look at other groups that are using the same working method. Janantha Marasinghe volunteered to help with the modification of the documents and was, since he has experience of developing similar working procedures, asked to send an example of this to the IR WG email list.

Action 01-06:
Janantha Marasinghe to send an example of relevant working procedures to the Incident Response Working Group email list.

- *Janantha* suggested that the Working Group keeps a repository of incidents in order for the incident managers to know if similar incidents have occurred before and possibly adopt a similar procedure. The Chair agreed.

- The Chair suggested that the Working Group should investigate what contact list there are for ccTLDs. The information will be compiled after the Seoul meeting and the Chair agreed.

- *Otmar Lendl* noted that since the IR WG might not be able to handle all upcoming security issues. It is therefore important to distinguish between incidents that directly impact the DNS, which are considered to be responsibility of the ccTLD , and other incidents, which are responsibility of other entities. In the work plan a good structure for delegating the different issues to the right people is essential. This structure should also include the differences per territory in this respect.

- The importance of a reliable and secure contact channel between the ccNSO and the ccTLDs in respect to incidents was noted and it was pointed out that only the people and processes affected by a certain incident should be involved.

- The group reached the conclusion that the Draft Plan needs to be more specific on what sort of issues the IR WG would handle and what threats there are to the DNS.

- *Eric Iriarte* suggested that the IR WG reaches out to the security workshops supported by the Regional Organisations and ICANN.

6. AOB

- Since some Working Group members arrive in Seoul on 25 October they will have trouble reaching the IR WG meeting in time. Kristina Nordström was asked by the Chair to look into a possible adjustment in the agenda, moving the meeting from 6pm to 8pm local time.

Action 01-08:
Kristina Nordström to look into the possibility of moving the IR WG F2F Seoul meeting on 25 October from 6pm to 8pm local time.

- *Kristina Nordström* informed the group that a Wiki Workspace will be available for the IR WG shortly. She also announced that it is possible to start using Adobe Connect Rooms as an addition during the telephone conferences.

7. Adjourn