Incident Response Working Group Telephone Conference

13-01-2010

Attendees:

Fahd Batayneh, .jo
Wim Degezelle, CENTR (Observer)
Luis Diego Espinoza, .cr
Ondrej Filip, .cz
Katrina Sataki, .lv
Jörg Schweiger, .de (Chair)
Zoran Vlah, .hr

ICANN Staff:

Yurie Ito, Director, Global Security Programs
Kristina Nordström, ccNSO
Save Vocea, Regional Liaison Asia-Pacific

Apologies:

Ben Fuller, .na
Paul McKitrick, .nz

- The Chair welcomed everybody to the call.

- The Chair asked the group for comments on his suggested amendments to the Work Plan. *Katrina Sataki* informed everyone that she prior to the call sent out comments to the list with suggestions on how to move forward. She stressed that she agrees that it would be of importance to define what would be considered an incident. She further noted that the Work Plan needs development. The Chair pointed out that setting up principles and action plans would be much easier to do with a definition of what an incident is. He asked the group for comments on whether or not a definition is necessary. *Wim Degezelle* replied that he considers a definition important since it is directly related to knowing when the Working Group should take action. The Chair asked the members to post any amendment suggestions on the email list.

- The Chair referred to a paper written by Olof Kolkman that classifies possible threats to registries and offered to send it out to the group. He encouraged members to post comments to the paper on the list for further discussion at the next meeting.

Action 03-01:
The Chair to send out a paper by Olof Kolkmans to the Incident Response Working Group members regarding possible threats to registries for further discussion on the next meeting.

- The Chair offered to compose a draft on defining what the Working Group should consider to be an incident, for further discussion at the next meeting.

Action 03-02:
The Chair to compose and distribute a draft on the definition of an incident for further discussion at the next Incident Response Working Group meeting.

- The Chair asked for other comments and suggestions to the Work Plan. No comments were noted. Due to that the IRWG work plan is adopted to the submitted version 2.1. He further noted a few points that needs attention:

  - Establishment of a repository that contains important information
  - A safe way of transferring information
  - Around the clock contact possibilities

  The chair pointed out that the "sophistication level" of the repository has to be defined and that the WG should comment to that on the list. *Yurie Ito* referred to a document with repository options that she sent to the Chair and suggested that it is distributed to the members for them to read and discuss it. She also mentioned that the costs for each ccTLD will be related to the extent of services the Working Group decides to offer. The Chair suggested that the document with repository options should be further discussed at the next meeting once everyone have had the chance to look at it.

Action 03-03:
The Chair to forward a document from Yurie Ito with repository options to the Incident Response Working Group members for further discussion at the next meeting.

- The Chair asked the members to look at point 3 in the Work Plan and jointly sort out the exact meaning of the sentence "Triaging requests and reports" with respect to who / what should accomplish this functionality (a system to be developed / SME's, …)

- *Luis Espinoza* suggested that the information repository should be closed to any outsider. He further suggested that a contact database is created with primary and secondary telephone numbers which is already specified within 1b (1) 5. and 6..

- The Chair noted that the Working Group should look at other similar organisations to make sure their respective tasks are not overlapping (with those stated for the IRWG. Already indentified related parties to look at were CERTS, DNS-OARC.

- The Chair referred to point 4 in the Work Plan and noted that the meaning of the term "Incident tracking" needs clarification and definition. He suggested that members submit comments about it on the list before the next meeting. It was unclear whether this is meant to be a globally (for the WG accessible) ticket system.

- *Wim* asked who would maintain the information in the repository, after is initial data set-up. The Chair replied that he is not sure but that he will ask Bart Boswinkel.

Action 03-04:
The Chair to contact Bart Boswinkel and ask him who would be responsible for the maintenance of the information in the repository.

- *Luis* noted that point 5 in the Working Plan is not complete.

- The Chair reminded the group about the Doodle poll still circulating the list regarding the face-to-face meeting in Nairobi. He further noted that the group should think about giving a presentation in Nairobi on the progress of the Working Group.

- The next Incident Response Working Group meeting will take place on 10 February at 12:00 UTC.

The meeting closed.