Incident Response Working Group Meeting in Nairobi

6 March 2010

Attendees:

Yuri Ito, ICANN
Jörg Schweiger, .de (Chair)
Bart Boswinkel, ICANN
Wim Degezelle, CENTR
Kristina Nordström, ICANN (telephone)
Greg Rattray, ICANN
Gabriella Schittek, ICANN
Zoran Vlah, .hr

Apologies:

Ondrej Filip, .cz

Working Group Work Plan

- The Chair noted that the Working Group needs to adjust its Work Plan so that it becomes more operational and reflects the Working Group's actual task. Following work plan was suggested:

- Definition of "incident" – by March 10th 2010
- Define use cases of the contact repository for ccTLDs – draft ready by April 30th 2010 (to be drafted by Yuri Ito)
- Define 'escalation procedures' and action paths – by May 30th 2010
- Define the repository data model to accomplish the use cases - Brussels meeting
- Suggestions to who will implement, run and maintain the repository at what level of acceptable expenditure, covered by whom – Brussels meeting + 1 month

No objections were noted to the proposed work plan

Definition of "Incident"

- The Chair felt that a slight refinement was needed to the current working group definition of "Incident". It was felt that the definition should be able to include new incidents such as the conficker attack, or other future attacks. He therefore presented a new suggested definition. It was felt that the third bullet point of the definition would be able to reflect new attacks:

"Large scale, unintended misfunction of the DNS or systematic, rigorous preparation of or actual attack on

- *the availability of the DNS or registratioin systems*
- *the data integrity or privacy of the DNS or registration systems*
- *the stability or security of the internet at large"*

- It was clarified that following cases would **not** be considered being an attack:

- the malicious use of the internet itself (such as SPAM)

- the unlawful use or misuse of specific domains/content (such as child pornography)
- any routing problems (such as BGP)

- The definition will be sent to the IR Working Group email list for consideration.

Contact Repository

- The Chair said it needs to be clarified who will be entitled to access the planned contact repository, and in which way. It should also be considered whether there is a need to secure the access of the repository to protect personal data and if so, what level of security is needed. The communication levels and methods needed for this should also be defined, as well as models on how the repository should be run.

- The Chair suggested to divide the use of the contact repository into three areas:

  - Information exchange purposes
  - Proactive actions against any attacks
  - Counter actions against attacks

  He asked the group for input. It was felt that the second point "proactive actions" needs further review and discussion amongst the working group members.

Definition of Escalation Procedures

- The Chair noted that the charter clearly states that the Working Group should formulate escalation procedures and action paths. However, he was not sure it would be very useful for the group to concentrate on this. He thought only a generic draft could be made, dealing with issues such as how to react according to best practices, how to get things organised and which peer groups already exists. The Chair said he would welcome input from the working group members, whether there already is a draft around which the group could build up on.

- *Yuri Itu* suggested that she could make a draft, if no other input is received. She said she would check what the escalation and response processes are for individual ccTLDs, as well as community wide escalation processes.

Related Initatives

- The Chair said the group needs to get a clear view of the delineation of the group's task versus already existing groups, which already play a certain role in the same area. He said the relation to groups such as DNS CERT or RSIGs need to be defined and how the work is related to DNS OARC's work. He also noted that the group needs to find out whether there are any related initiatives ongoing within the GNSO.

- *Greg Rattray* informed that VeriSign is leading a related initiative within the GNSO community. He offered to send out more information to the Incident Response Working Group on the issue.