Notes Incident Response Working Group Telephone Conference

29 April 2010

Attendees

Bart Boswinkel, ccNSO
Wim Degezelle, CENTR
Steven Deerhake, .as
Ondrej Filip, .cz
Otmar Lendl, ,at
Jörg Schweiger, .de (Chair)
Gabriella Schittek, ccNSO

Apologies

Paul McKitrick, .nz

Updated Charter

- The Chair informed the group that since there was no reaction from the Working Group to the suggested amendments to the charter, it was put forward to the ccNSO Council for adoption. The ccNSO Council had no objections. This means the amended Charter has been approved and will be posted on the website shortly.

- The Chair pointed out that some of the features in the Working Group's (new) charter have been overtaken by current actions: The Working Group was supposed to gather input from the ccTLD community regarding ICANN's DNS CERT initiative – however, the ccNSO has already submitted a formal comment to ICANN on the initiative. These comments were mainly based on discussions in Nairobi and on the email lists. The Chair therefore did not see a point in gathering further comments on the topic. He suggested that the next step would be to wait for ICANN's response to the community comments. Its then, to gather and summarize comments of the ccNSO community and to compile an answer/feedback (if needed) to ICANN.

  Bart Boswinkel clarified that the ICANN response should be published before the Brussels meeting.

Final Definition of "Incident"

- The Chair noted that some slight amendments were made after the Nairobi meeting. In detail the part about "misuse" was added. He felt that the definition is now perceived as clear and stable. However, he invited the group to submit final comments.

- *Steven Deerhake* wondered whether it would be an idea to include "WHOIS server issues" in the definition, as the .as registry is experiencing periodic attacks, which forces them to close down their port 43 service for short time periods.

  Some discussions followed, but it was felt that the WHOIS service rather is a part of the registry system and would not require any joint reactions to such incidents,

as such attacks would not majorly disrupt the functioning of the internet. It was therefore decided not to add it and to close the definition.

First Draft Contact Repository Use Cases

- The Chair reminded the group that it was agreed in Nairobi to invest some time in the definition and formulation of Use Cases for a Contact Repository. He pointed out that the draft, which was posted to the group prior to the call, was not complete. Input was still needed from Yuri Ito, who was tasked to look into the definition and formulation of Use Cases, but had not yet done so. It was felt there was no point discussing the draft before Yuri had submitted more information.

  Bart Boswinkel offered to contact Yuri to see if she has the time to draft something on the topic in time for the next Incident Response Working Group Call.

- The Chair said that he thought there were two core functions in the use cases that should be addressed: "Providing a Security Contacts" and "Informing the Participating Community About an Incidence". Other issues, such as "Generate a Report" was not perceived as being something the use cases should incorporate, be it just for the fact that the working group is of non-permanent nature. It was also felt this function could be done by some other entity. *Steven Deerhake* pointed out that "Proactive Actions" should not be a matter for the Working Group either. *It was agreed that* "Enable Security Support for Community Members" is part of the desired Use Cases.

Draft Contact Repository Data Model

- It was felt that the Use Cases list needed to be completed before the Group could start talking about the Contact Repository Data Model in detail. However, the Chair noted that *Gilles Massen* had suggested adding two additional data points: alternative contact name and authentication information.

- *Steven Deerhake* added that he would also like to see the contact person's default time zone, as well as the office hours for the contact person.

- *Ottmar Lendl* suggested adding encryption keys to the authentication information.

Consider and Adopt Existing Work from DNS-OARC

- The Chair said that when reading the DNS-OARC Executive Board's comments on DNS CERT, he realised that the organisation might have a database/repository scheme in place that the Working Group is looking for. He therefore suggested that the group should have a look at DNS-OARC's structure and see whether it could be useful. He asked the Working Group members if they could help in investigating .

- *Ondrej Filip* said DNS-OARC is meeting in Prague that weekend and that he is willing to contact the organisation. The Working Group Chair considers to attend the meeting as well.