



Incident Response WG – Status

Joerg Schweiger

WG Chair <ccnso-erpgw@icann.org>

<schweiger@denic.de>

Cartagena, December 2010, ICANN ccNSO Meeting



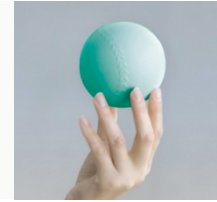
Purpose

- assist in implementing sustainable **mechanisms for the engagement of and interaction with ccTLD registries during incidents** that may impact the **DNS**

Scope

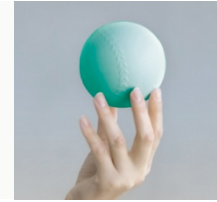
- repository of ccTLD contacts and channels of communication for incident response

Work plan



✓	1. Define what is considered to be an <u>incident</u>	March, 10 th
✓	2. Define the <u>use cases</u> of the contact repository for ccTLDs	April, 30 th
✓	3. Define escalation procedures and action paths	May, 30 th
✓	4. Define the repository <u>data model</u> to accomplish the use cases	Brussels meeting (June)
	5. (Towards the) Implementation of the contact repository <ul style="list-style-type: none">• Make or Buy?• Suggestions to who will run and maintain the repository at what level of acceptable expenditure covered by whom	Cartagena
+	See to the discussions referring to the DNS-CERT initiative	since Nairobi

→ Next steps



Buy

- **Trusted Introducer**
 - meets / could easily be adapted to the contact repository's data model and use case requirements
 - browse through a list of alphabetically listed contacts
 - ➔ data is kept up-to-date by the operator
 - „secured“ email communication
 - „Internet-based“ communication and voice mail and SMS
 - redundantly operated in 2 data centers
 - per participant: 1,400 \$ p.a. + (one time) set up fee: 1,300 \$
 - used by CSIRTs
- **Packet Clearing House tool**

Make

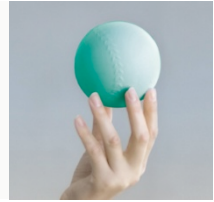
- „browse“ or „query“ solution (resulting in different look & feel and maintenance models)



Functional and non-functional „must-have“ requirements

- Support the envisioned use cases
- High availability 24/7
- Alternative communication channels (not using the internet)
- Data is kept up-to-date

¿ Anything else ?



Further steps can't be done nor decided by the WG (alone) ...

- Make or buy decision and sophistication level of the contact repository implementation heavily depends on financing abilities
 - Completely covered by ICANN
 - ICANN covers implementation, each participants pays for operational cost
 - Cost per participant is completely covered by the respective participant
 - Sponsoring models
 - Fixed pricing no matter how many participants
 - ...



Further steps can't be done nor decided by the WG (alone) ...

Decisions?!

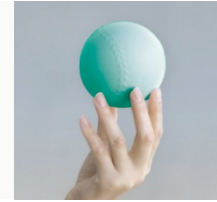
1. The ccNSO council / ICANN to suggest and seek input from the community on financing
2. The ccNSO council / ICANN to task further examination, selection and implementation given the framework of data model, use cases and must-have requirements
3. Close down the IR WG



Backup



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



Incident

Large scale, unintended malfunction 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



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 mitigation lessons learned
- Provide generic action plans ➡ reflect this in the charter
- Coordinate responses

➡ Work plan

Work plan action item 3: Contact repository data attributes



<ul style="list-style-type: none">• Internet domain• ccTLD operator name• Host organization of ccTLD response contact point• Registry operator name	
<ul style="list-style-type: none">• Name of person representing the team• Function/role of the person• Authentication 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	<ul style="list-style-type: none">• Name of substitute person representing the team 

→ Work plan

Questions?



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