



Incident Response WG – current status

Joerg Schweiger

WG Chair <ccnso-erpgw@icann.org>

<schweiger@denic.de>

Nairobi 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
- **qualification of**
 - incidents
 - escalation procedures
 - action paths



Work plan

1.	Define what is considered to be an incident	March, 10 th
2.	Define the use cases of the contact repository for ccTLDs	April, 30 th
3.	Define escalation procedures and action paths	May, 30 th
4.	Define the repository data model to accomplish the use cases	Brussels meeting
5.	Suggestions to who will implement, run and maintain the repository at what level of acceptable expenditure covered by whom	Brussels + 1 month



Definition: Incident (to be revised frequently)

Systematic, rigorous preparation of or actual attack on

- the availability of the DNS or registration systems → DDOS, EPP flaw exploit
- the data integrity or privacy of the DNS or registration systems → Zone enumeration, cache poisoning, social engineering
- the stability or security of the internet at large → was: conficker; will be: ???

where a coordinated international response by operators and supporting organisations is advised.



Considered **not** 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, ...)



1. Contact repository - Sophistication requirements ?

- Who is entitled to access?
- Needed security level of access and communication means?
- Hosted by a professional third party or dedicated ICANN branch or just an IANA database extension?

2. Escalation procedures and action paths

- Definable in a useful way or “just generic”?

3. Relation / Delineation with respect to existing organisations obliged with related or similar tasks

- DNS-CERT, DNS-OARC, SSAC, RSIG, CERTs/CSIRTs, FIRST, BTF, ISC SIE, gTLD-initiative?

Questions?



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





Contact repository data attributes (first draft)

- ccTLD name
- Name of person representing the team
- Host organization of ccTLD response contact point
- Country the contact is located
- Internet domain
- Regular telephone number (country code, telephone number,time-zone relative to UTC):
- Emergency telephone number (country code, telephone number,time-zone relative to UTC):
- Email address
- Messenger services (service, id)
- Facsimile number (country code, fax number)
- Other telecommunication facilities
- Language



Use cases (first draft)

- **Information exchange**
 - Provide a security contact point under any circumstances
 - o Generate reports on prevention best practices (technical, process related)
 - o Store/compile/give access to mitigation lessons learned

- **Proactive actions**
 - Provide generic action plans
 - o Generate reports on potential threats

- **Counter action**
 - o Inform the “participating community” about “an incident”
 - o Coordinate responses
 - o Facilitate/enable community support for „a community member“