CCoP : CSIRT Code of Practice

Don Stikvoort – m7 partner

CCoP version 3.0

Friday 13 May 2016

Is this the face of evil ?

CCoP background

- Our ethics are not all the same
- People will do weird things, by all standards
- People will do weird things, by professional standards
- But what are the standards?

- Parker/Cormack/Maj/Stikvoort drafted CCoP
- 2005 ➔ Version 2.1 approved by TI accredited teams
- SHOULD criterion = strong recommendation
- 2009 ➔ SIM3 parameter H-1 : Code of Conduct/Practice/Ethics
- Starting point for discussion

11 years old

v2.1 of 2005 needed update

- The world and the net are a different place
- Team who wanted to charge a peer for basic CSIRT work
  - Not in the CCoP
- Time for an update anyway
  - Experience from setting up teams and doing certifications

And so ?

v2.1 → v3.0

- "Definitions"
  - CSIRT more widely defined
  - Add "team members"
  - Use RFC definition for MUST and SHOULD
- Add "Starting Points"
  - CSIRTs work peer-to-peer without cost recovery
  - Clarification of "peer"
  - Benefit of the doubt for valid reporters
- "Legal Requirements"
  - Transparency in legal aspects a la rfc-2350 ???

v2.1 ➔ v3.0

- "The Team"
  - Added: "The team will, considering its stated services towards its constituency, take appropriate incident management action when it is notified of an incident in its constituency."
- "Team Members"
  - No changes except clarification throughout on team vs staff
- "Information Handling"
  - Terminology improvements only
- "Service Specific Requirements"
  - Modular approach dropped, content kept and improved ➔
  - "Vulnerability Handling Requirements"

v2.1 ➔ v3.0

- "Vulnerability Handling Requirements"
  - New: "The team SHOULD encourage the adoption and use of managed disclosure practices."
  - New: "Any public disclosure of what could be considered critical vulnerabilities should not only follow the guideline of 7.4, but also the team should seek to achieve a coordinated effort within the CSIRT community – and especially any such disclosure should be done as a concerted and synchronised effort."

Pre-amble

THAT’S IT FOR NOW FOLKS

SEE YOU IN ZÜRICH