Tipsi in Europe

An objective basis for CERTs in Europe: the foundation for the establishment and maintenance of the CERT web-of-trust.

Klaus-Peter Kossakowski & Don Stikvoort

M&I/Stelvio, by commission of TERENA

Info@stelvio.nl

Situation Report (i)

- Organisations slowly build up CERT capability (3 phase model in report)
- US few years ahead
- 90 FIRST members worldwide
- 27 FIRST members in Europe
- Hundreds of CERT capabilities will arise in the years to come

Situation Report (ii)

- The pub-model of trust is outdated:
  - Too many teams
  - People change jobs too often
  - Financial stakes have become too high
- The mentoring-model cannot cope by lack of mentors and set rules
- “Today’s approach is not reliable, does not scale, …”
Situation Report (iii)

- FIRST will not solve this problem in the next few years
- Neither will ISOC or IETF
- Nor will Law Enforcement
- TERENA is well suited to launch a solution in Europe
- “trusted introduction” is the way – certification is still a bridge too far

Scope

- Europe +
- ISP teams
- Government related teams
- Vendor (product) teams
- Teams for major international companies or institutions
- Major commercial CERT providers

Deliverable

- Describe an objective basis for CERTs in Europe: a foundation for the establishment and maintenance of the CERT web-of-trust
- Objective Criteria and Process
- Trust to be replaced by Expectations
- Process to be implemented by a “Trusted Introducer”, a coherent entity
Paradox

The Trusted Introducer can only generate trust if it bans trust from its proceedings and only concentrates on authentic CERT-team statements. Trust resides at the CERT level only.

CERT-team Statement

Properties

• Authenticity
  – Essential quality with regards to trust generation

• Actuality
  – Essential for trust maintenance

• Correctness
  – CERT-scene not yet ripe for certification

CERT levels

• Level 0 = team is within scope
• Level 2 = authentic standardized team information available, including logs on the establishment of this information and its authenticity
• Level 1 = temporary intermediate phase
Criteria (i)

i. Teams MUST be described by a filled in “Appendix E”, that will be published on a private website

ii. Teams MUST cooperate with the publication of essential data on a public website

iii. Teams SHOULD adhere to RFC 2350

iv. Teams MUST maintain the info provided

Criteria (ii)

v. Teams MUST support site visits when necessary

vi. Teams MUST do PGP or alike (unless forbidden by law)

vii. Teams MUST support QA sessions with the Trusted Introducer

viii. Teams SHOULD attend relevant meetings and conferences

Process (i)

**TASK 1** =

- Initial quick scan of teams inside Europe
- Maintain that list
- Advertise process etc on public website, meetings etc.
- Needs experienced staff
Process (ii)

TASK 2 =
Establishment of Level 1 teams
• Invite “suitable” teams to become level 1
• “Suitability” decided purely on basis of
formal requests, or assessment by the
Trusted Introducer
• Team will have to meet all MUST criteria
and seriously look into the SHOULDs
within 3 months

Process (iii)

TASK 3 =
Establishment of Level 2 teams
• If all MUST criteria have been met and
have proven to be authentic and
representative of the team or its parent
organisation, then Level 2 applies
• All data available on private website

Process (iv)

• ESSENTIAL is the gathering of when-
from whom - how - what information about the
collected team data
• This value-added – though objective ! –
information is an important basis for the
(de)generation of trust : it’s the information
between the lines
• Trust is a matter for the teams – to set
documented expectations is the goal for the
Trusted Introducer
Process (v)

**TASK 4 –**
Maintenance of Level 2 Status
- Trust takes years to gain but is lost overnight
- Level 2 teams MUST inform the Trusted Introducer of any changes in the data they provided

Process (vi)

Review Board for Trusted Introducer
- Review Trusted Introducer’s work
- Set policies
- Escalation authority (decide on site visits, exceptions to timelines and rules, etc)

Implementation (i)

- **FIRST:** currently not equipped
- **TERENA:** not in the web-of-trust
- Informal set of CERT-teams: continuity and stable quality at risk
- Subcontraction: best possibility
  - needs neutral focal point inside web-of-trust, both regionally and internationally
  - **TERENA** to facilitate funding and oversight
Implementation (ii)

- Cost recovery by annual Level 2 fee
  - Partial recovery by e.g. Euro 200 fee
  - Full recovery will need "initially" higher fee (example: appx 1000 Euro per team per year for 10+ Level 2 teams; but only 100 Euro with 100+ teams)
- Invited site visits paid for by inviting sites

Recommendation

- TERENA to subcontract Trusted Introducer function to suitable party
- Use leftover money from EuroCERT to gain initial momentum by avoiding high annual fees because of initial lack of paying customers
- Go for 25+ Level 2 teams within 2 years and financial self-support of the service
- Clearly distinguish between private services (paying customers only) and public ones