Panel session on 'Cyber Security Standardisation'

Demosthenes.Ikonomou@enisa.europa.eu

ENISA

Vienna, April 7, 2014 (13.45 - 15:45)

ENISA and International Standardisation Organisations (ISO)

- Part of ENISA's mandate (Article 3.g)
  - To ***'track the development of standards'***;

- Part of the EC Cyber Security Strategy:
  - To ***'Develop, in cooperation with relevant national competent authorities, relevant stakeholders, International and European standardisation bodies and the European Commission Joint Research Centre, technical guidelines and recommendations for the adoption of NIS standards and good practices in the public and private sectors.'***.

ENISA and ISO – so far

- Established collaboration agreements with:
  - ISO SC27
  - ETSI (MoU)
  - CEN CENELEC (MoU);
- ENISA aligns key activities with the work of ISO
  - ETSI TISPAN on CIIP
  - ETSI LI on DRD
  - CEN CENELEC on smart grids;
  - ETSI on Cloud certification;
  - ISO SC 27 in the area of privacy;
- Also a member of the ETSI CEN-CENELEC Cyber Security Coordination Group;

ETSI, CEN, CENELEC Cyber Security Coordination Group (CSCG)

- Co-ordination Group of the three European Standards Organizations (ESOs) CEN, CENELEC and ETSI
  - Since December 2011
- Experts from ESOs of 14 EU MS
- Together with European Institutions (ENISA, EC/JRC)
- Chaired by Dr. Christian Ehler, German MEP
- Supported/Secretariat by DIN, Germany

CSCG Terms of Reference (ToR)

- To act as contact point for all questions of EU institutions relating to standardization of cyber security
- To provide strategic advice on Cyber Security to ESOs
  - Analyze and provide joint guidance on Cyber Security Standards
  - develop a gap analysis of European and International Standards on cyber security
  - define of joint European requirements for European and International Standards on cyber security
- establish a European roadmap on standardization of cyber security
- Co-ordinate Standards with others (including NIST and USA)

CSCG deliverables

- Security white paper
  - Recommendations for a Strategy on European Cyber Security Standardisation
  - Started in December 2012
  - Approved by ESOs (Q4/2013)
- Provides input to European Commission activities, includes ESOs proposed roles
- Mentions proposed method of working, activities

CSCG White Paper (1 of 2)

- Propose the creation of a governance framework for the coordination of Cyber Security standardisation
- launch an initiative to re-establish the trust
- European Public Key Infrastructure and strong cryptographic capabilities
- establish a clear and common understanding of the scope of Cyber Security

CSCG White Paper (2 of 2)

- high-level European Cyber Security Label
- extend existing European Cyber Security requirements and evaluation frameworks
- create a high-level interface between the CSCG and the European research community
- launch a targeted global initiative to promote standards appropriate to European requirements
- Next steps?
  - Industry involvement.

Challenges (from an EU perspective)…

- Need establishing a small number of key initiatives at EU level ('Airbus'-like projects)
  - Multi-disciplinary projects with industrial participation;
  - Necessary contributions by DPAs, apps developers;
  - H2020;
- Improve coordination between EU funded R&D and ISO;
- Possible 'vehicles' for such a coordination
  - ETSI CEN CENELEC CSCG;
  - H2020 (industrial platforms);

Open questions…

- Are current initiatives adequate to address the issues?
  - If not, what other is needed?
- How to transpose the high level objectives of the CSCG and relevant policy documents (e.g. NIS CSS) into projects and to the market (regulatory initiatives)?
- Industrial involvement??
  - Research (e.g. H2020), regulation, etc.?
  - Are standardisation mandates the best (or an appropriate tool)?
- Are current practices sufficient/working?
  - If not, what needs to be done differently?
- Is there a role for the public sector (e.g. procurement, certification, etc.)?

Panel Session

- Prof. Reinhard Posch, Head of the Institute für Angewandte Informationsverarbeitung und Kommunikationstechnologie (federal CIO for the Austrian government);
- Prof. Bart Preneel, Katholieke Universiteit Leuven.
- Ilias Chantzos , Symantec, Senior Director, Government Affairs EMEA, Global CIP and Privacy Advisor