ENISA activities in standardisation

Dr. Andreas Mitrakas
ETSI Security Week – Sophia Antipolis, 12 June 2017

European Union Agency for Network and Information Security
Positioning ENISA activities

HANDS ON

MOBILISING COMMUNITIES

POLICY IMPLEMENTATION

RECOMMENDATIONS

ENISA activities in standardisation | Dr. Andreas Mitrakas
### Strategic threat landscape 2016

<table>
<thead>
<tr>
<th>Top Threats 2015</th>
<th>Assessed Trends 2015</th>
<th>Top Threats 2016</th>
<th>Assessed Trends 2016</th>
<th>Change in ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Malware</td>
<td>🔄</td>
<td>1. Malware</td>
<td>🔄</td>
<td>→</td>
</tr>
<tr>
<td>2. Web based attacks</td>
<td>🔄</td>
<td>2. Web based attacks</td>
<td>🔄</td>
<td>→</td>
</tr>
<tr>
<td>3. Web application attacks</td>
<td>🔄</td>
<td>3. Web application attacks</td>
<td>🔄</td>
<td>→</td>
</tr>
<tr>
<td>4. Botnets</td>
<td>🔄</td>
<td>4. Denial of service</td>
<td>🔄</td>
<td>↑</td>
</tr>
<tr>
<td>5. Denial of service</td>
<td>🔄</td>
<td>5. Botnets</td>
<td>🔄</td>
<td>↓</td>
</tr>
<tr>
<td>6. Physical damage/theft/loss</td>
<td>🔄</td>
<td>6. Phishing</td>
<td>❌</td>
<td>↑</td>
</tr>
<tr>
<td>7. Insider threat (malicious, accidental)</td>
<td>🔄</td>
<td>7. Spam</td>
<td>❌</td>
<td>↑</td>
</tr>
<tr>
<td>8. Phishing</td>
<td>❌</td>
<td>8. Ransomware</td>
<td>❌</td>
<td>↑</td>
</tr>
<tr>
<td>11. Data breaches</td>
<td>❌</td>
<td>11. Exploit kits</td>
<td>🔄</td>
<td>↓</td>
</tr>
<tr>
<td>12. Identity theft</td>
<td>❌</td>
<td>12. Data breaches</td>
<td>🔄</td>
<td>↓</td>
</tr>
<tr>
<td>13. Information leakage</td>
<td>🔄</td>
<td>13. Identity theft</td>
<td>❌</td>
<td>↓</td>
</tr>
<tr>
<td>15. Cyber espionage</td>
<td>🔄</td>
<td>15. Cyber espionage</td>
<td>❌</td>
<td>→</td>
</tr>
</tbody>
</table>
The standardisation framework for ENISA

- Regulation 526/2013, “Support research and development and standardisation, by: facilitating the establishment and take-up of European and international standards for risk management and for the security of electronic products, networks and services”

- NIS Directive: “ENISA, [...] shall draw up advice and guidelines regarding the technical areas [...] as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered”

- Regulation 460/2004: “the Agency shall [...] track the development of standards for products and services on network and information security”
Collaboration with SDOs

• **Established cooperation with:**
  – ISO SC27 (Liaison)
  – ETSI (MoU)
  – CEN CENELEC (Collaboration agreement)
  – ITU SG17

• **Technical collaboration:**
  – ETSI TISPAN on CIIP
  – ETSI ESI on eID
  – ETSI CLOUD on cloud certification
  – CEN CENELEC on smart grids
  – ISO SC 27 in the area of privacy

• **Active member of CSCG** (CEN-CENELEC Cybersecurity Focus Group)
  – Providing advice on CSCG actions
  – Receiving advice on ENISA projects
  – Common deliverables
Standardisation – select deliverables

• In cooperation with CSCG
  — Definition of Cybersecurity – Gaps and overlaps in standardisation
  — Governance framework for European standardization

• General standardization papers
  — Gaps in NIS standardization – Recommendations for improving NIS in EU standardisation policy
  — Information security and privacy standards for SMEs

• Publications in relation with eIDAS Regulation
  — Standardisation in the field of Electronic Identities and Trust Service Providers
  — Analysis of standards related to Trust Service Providers – Mapping of requirements of eIDAS to existing standards
  — Recommendations for TSPs based on standards – Technical guidelines on trust services
Work Programme 2017

• O.1.3.1 – Guidelines for the European standardisation in the field of ICT security

“This activity will provide an assessment of the situation of European standardisation in the area of ICT security, taking into account the new requirements and priorities associated with the NIS Directive (and potentially the Commission’s communication on cPPP). It will analyse the gaps and provide guidelines for, in particular, the development of standards, facilitation of the adoption of standards and governance of EU standardisation in the area of ICT security.”

• Deliverable
  – Assessment of implementation of standards in MSs and their support for NIS regulations and policies
  – Overview of available NIS standards for IT products, systems and services
  – Identification of factors limiting or reducing adoption
  – Opinion on NIS related standards.
  – Identification of gaps in NIS standardisation
  – Conclusions and recommendations for the future development of standards in the NIS area
1st Annual CSCG / ENISA Workshop

- **Goals:**
  - Approach to coordination of Cybersecurity standardization activities
  - Putting together
    - MS policy makers
    - EU institutions (CNCT, GROWTH, JUST, HOME, RESEARCH, JRC)
    - SDOs
- **Areas to be covered:**
  - Standardisation in Support of EU Policy
  - Privacy and Data Protection
  - European Cybersecurity Label and Assurance
  - Norms for the Internet of Everything
- **Practicalities:**
  - 19th September 2017, 8:00-18:00
  - Brussels, CEN/CENELEC, av. Marnix 17
Certification

- **Challenges from the EU perspective**
  - Recognition of trustworthiness of security products requested by EU legislative initiatives (eIDAS, NIS, GDPR)
  - No common EU Framework

- **Existing initiatives**
  - National efforts
  - Cross country initiatives
  - SOG-IS Mutual Recognition Agreement
    - The MRA is not part of the “EU acquis”
    - The MRA does not apply to the 28 Member States

- **ENISA actions**
  - Workshops on certification (MS and industry), since February 2016
  - Collaboration with the EC on the roadmap for a common framework of certification of security products and within cPPP
  - Collaboration with members of the semiconductors industry (joint paper published in December 2016)
Thank you

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu