CSIRTs network

Andrea Dufkova | CSIRTs-relations
NLO meeting | Athens, GR | 26th April 2017

European Union Agency for Network and Information Security

NIS Directive and CSIRTs

- **Article 9** of the Directive gives the framework for CSIRTs

- **Article 12** of the Directive covers the CSIRTs Network

- **Annex 1.** Requirements and tasks of the CSIRT. This Annex gives a list of tasks that a MS' CSIRT has to perform

- **Annex 2.** Sectors and entities. This Annex lists the sectors and subsectors that need to be covered by each country's Information Security Strategy and CSIRTs

ENISA's overall role and contribution

- Assist MS and EU Comm by providing expertise/advice and by developing/facilitating exchange of good practices, e.g.

- ➢ **Be the secretariat of the CSIRT network and develop with members the network**

- Participate/contribute to the work of the Cooperation Group (CG)

- Elaborate advices and guidelines regarding standardization in NIS security, together with MS

CSIRTs network update 2016 – 2017/Q1

Overview:

❑ Statutory documents

❑ Secretariat

❑ Active support

Statutory documents

- The Work Program describes **a set of goals** for the CSIRT Network required in which relevant information can be exchanged in accordance with art. 12 of the Directive.

- As the CSIRT Network **success** depends on several factors; **four elements**, preparatory work, as well as short, mid and long term goals.

- Preparatory tasks consist of **fundamental requirements** for a **successful launch** of the CSIRT Network in February 2017.

- **Short-, mid-, and long-term goals** on the other hand define tasks for each of the three reporting terms.

- Importantly the set of tasks for each reporting period needs to be seen as a **non binding guideline** that needs additional specification and continuous adjustment.

✓ Short Term Goals (Q1/2017 – Q3/2018)

Theme: "Developing trust and confidence between CSIRTs"

Strategic Goals: e.g. Approve statutory documents, define SOPs, support service needs, functional exchange with CC, etc.

- ✓ 30%

- ✓ 40% kicked-off

(five WGs established: on building functional exchange with CC, on SOPs, on Security requirements for Services, on Network Portal and on CSIRT maturity assessment)

- ✓ 30% not started, but scheduled

Operational Goals: e.g. Establish internal contact directory, Create and maintain a private web portal and collaboration space, Adopt TLP based approach for IX, etc.

- ✓ 40%

- ✓ 40% kicked-off (Portal)

- ✓ 20% not started, but scheduled

Tactical Goals: Trust building, team building event, mutual assistance, first stock taking on team description, trainings, etc.

- ✓ 40%

- ✓ 40% kicked-off (WGs and Portal)

- ✓ 20% not started, but scheduled

Secretariat

- ✓ ENISA provides the secretariat and actively supports the cooperation among the CSIRTs

- ✓ <u>The secretariat will be notified of appointment and changes by the national standing representatives.</u>

- ✓ The secretariat supports the functioning of the network by (e.g. rooms, events, video-conf facility, mailing list, portal, etc.)

  - ✓ Portal set up and actively used since Q1/2017
  - ✓ Mailing list since Q2/2016
  - ✓ 3 informal preparatory meetings took place in 2016
  - ✓ 3 formal meetings scheduled in 2017 (February/Malta; May/Estonia; Q4/tentative)

- ✓ the Chair trio draft a report to the Cooperation Group once every 18 months, with assistance of the Secretariat

Active support

Good practice guidelines and methodology on different CSIRT topics

➢ **CSIRT maturity assessment**

  ➢ (Work in progress since 2010; currently on CSIRT maturity assessment criteria and peer-review methodology)

➢ **CSIRT common taxonomy for information sharing**

  ➢ (Common taxonomy for the classification of incidents within the National Network of CSIRTs)

➢ **CSIRT training material**

  ➢ (Stock taking of Existing Training Schemes in NISD Sectors)

➢ **CSIRT Handbook**

  ➢ (Guidance on forming and operating a CSIRT. In particular, how to define and document the nature and scope of a IH service, etc.)

Thank you

🏠 PO Box 1309, 710 01 Heraklion, Greece

📞 Tel: +30 28 14 40 9710

✉️ info@enisa.europa.eu

🌐 www.enisa.europa.eu