December 2016 (SK – MT – NL)

CSIRTs Network
Terms of Reference and Rules of Procedure

Terms of Reference

- The CSIRTs Network is established through the NIS Directive (EU) 2016/1148, which sets the scope of the activities of the CSIRTs Network.[1] The CSIRTs Network will operate in parallel to existing networks of CSIRTs, both within and outside the EU. The unique characteristic of the CSIRTs Network is that it involves all EU Member States and CERT-EU, and is therefore well-positioned to enhance trust and cooperation across the Union. The creation of a solid trusted network in which relevant information is exchanged between all CSIRTs in accordance with art. 12 of the Directive should be one of the primary focus areas.
- The CSIRTs Network is a network composed of EU Member States' appointed CSIRTs and CERT-EU ("CSIRTs Network members"). The Commission will participate in the network as an observer. ENISA will provide the secretariat and shall actively support the cooperation among the CSIRTs.[2]
- In regular CSIRTs Network meetings, a Member State and CERT-EU will be represented by two, with a maximum of three, representatives (two standing and one other). Ideally, these representatives are appointed for a longer period for the purpose of creating stability and building trust. The secretariat will be notified of appointment and changes by the national standing representatives.
- All CSIRTs Network members should receive all information shared within the context of this network. Information is brought to the network by all CSIRTs Network members and members are encouraged to a timely sharing of information related to challenges and threats to improve the EU-wide preparedness.
- Incidents cooperation and coordination is on a voluntary basis.[3]
- The CSIRTs Network is an European internal cooperation and coordination network. It does not constitute any kind of (corporate) body or entity. Hence the CSIRTs Network is not an alternative to bilateral or multilateral CSIRT-to-CSIRT contact and is not intended to replace existing multilateral CSIRT cooperation arrangements, nor limit forming and developing other multilateral arrangements, both within and outside the EU.
- If the CSIRTs Network faces issues or envisages to take actions with a political or strategic dimension, or any other matters outside of its main agenda, it will require guidance from the Cooperation Group.

Rules of Procedures

Budget

The budget of the CSIRTs Network should be a combination of:

- Funding by each Member State for, but not limited to, the costs for participation in the network, including representative/expert in the CSIRTs Network;
- ENISA, as secretariat of the network, to support the functioning of the network (e.g. rooms, events, etc.);
- Specific financing mechanisms (e.g. CEF).

Rules of information sharing

- TLP based approach.
- No exchange of classified information (as long as no appropriate facilities and agreements are in place).

---

1 Article 12 of the Network- and Information Security Directive

2 Article 12.2 of the Network- and Information Security Directive

3 Article 12.3 of the Network- and Information Security Directive

Decision-making process

- The primary decision-making mode is consensus.
- Without prejudice to the voluntary nature of the network, procedural matters are decided upon by Qualified Majority Voting[4], whereby each Member State and CERT-EU have one vote (regardless of the number of CSIRTs Network members in their national delegation).

Sanctions

No sanctions for CSIRTs not cooperating.

Use of external sources of information (e.g. other mechanisms)

- Every CSIRTs Network member should be responsible for providing the information to the network it deems relevant.
- The CSIRTs Network itself should not require nor pay for access to external sources of information.
- The CSIRTs Network should, where possible, use knowledge and expertise of existing networks of CSIRTs (e.g. TF-CSIRT and FIRST).
- The CSIRTs Network should, where possible, use knowledge and expertise of the private sector on a European level (e.g. existing European ISACs).

Link to other EU agencies (e.g. EC3)

The CSIRTs Network is not an EU agency and should not liaise as such with other (EU) agencies (see Terms of Reference). Representatives of agencies might nevertheless be invited to share information with the CSIRTs Network to specific meetings and/or specific agenda items, on a strict *ad hoc* basis. Vice versa, EU agencies may invite CSIRTs Network members to share their experience. The sharing of operational information between Member States and EC3 should primarily go via the national law enforcement channels.

International contacts

As the CSIRTs Network is an European internal cooperation and coordination network and does not constitute any kind of (corporate) body or entity (see Terms of Reference), thus the CSIRTs Network:

- Should neither seek to establish international contacts
- Nor constitute an international POC by default for contacts between CSIRTs from inside nor outside the EU.

In case a CSIRT from outside the EU would seek to contact one or several EU Member States CSIRTs or CERT-EU by contacting the CSIRTs Network, the Chair shall invite the other CSIRT to contact the respective CSIRTs directly (and if necessary provide their contact information) using a regularly updated directory (that the network's Secretariat might manage). Requests for presentations, incoming and outgoing, will be handled by the Chair and the Secretariat.

Exercises

The CSIRTs Network should be able to conduct internal exercises to test the processes established (e.g. directories, technical SOPs, etc.) and improve its functioning. Such exercises could as well be part of the Cyber Europe framework. Nonetheless, prior to conducting exercises, the basis for operational cooperation should be established.

Procedures

The CSIRTs Network defines procedures for the purpose of an incident. These procedures could be based on the EU Standard Operating Procedures (SOPs) that were developed within the Cyber Europe Exercise Framework.

[4] http://www.consilium.europa.eu/en/council-eu/voting-system/qualified-majority/

Tools and hosting of tools (e.g. information exchange platform)

- When choosing the tool(s) that will support its activities, the CSIRTs Network should on the short term select simple and practical tool(s) allowing it to function as soon as possible.
- As a consequence, priority should be given to tools allowing swift information exchange among CSIRTs, while keeping in mind that additional and more sophisticated tools can be added in the future (step-by-step approach).
- When choosing the most appropriate tool(s), the CSIRTs Network should assess and choose among available solutions (e.g. the soon to be set up CEF CSIRT platform, ENISA Cyber Europe web platform, other existing tools), according to previously mentioned principles and before considering developing new tools.
- The setting up of a web platform for non-sensitive information exchange hosted by ENISA could be envisaged. Any new information platforms should be discussed and agreed within the CSIRTs Network.
- Hosting of tools is preferably a combination of centralized and decentralized components.
- In case the tool(s) would be centrally hosted or both centrally and decentrally hosted, voluntary Members or both voluntary Members and ENISA could act as hosts.

Chair

- The CSIRTs Network is chaired by representatives from the Member States' CSIRTs.
- The chairing is based on the Presidency calendar of the Council of the EU, including a rotation every 6 months.
- The process of designation of the representative is at the discretion of individual Member States. Nonetheless, the representative should be a recognized member of the CSIRT Community and preferably (one of) the standing national representative in the CSIRTs Network.
- The chairing of the network should be based on a Chair trio (Troika) consisting of:
    - The Chair
    - Two alternates: the previous chair and the next Chair.
- The Chair shall be assisted in the performance of his duties by representatives of the Member States holding the previous and the following Presidency of the Council of the EU.
- Tasks of the Chair should, amongst others, be to:
    - Draft an action plan
    - Set, with its alternates, the goals for 18 months, keeping in mind the previous goals
    - Determine the agenda
    - Provide instructions for the Secretariat tasks
    - Stimulate active participation by all CSIRTs Network members
    - Report to the Cooperation Group
    - Liaison to the Cooperation Group
    - Upon invitation and where relevant participate in meetings in EU fora (e.g. Horizontal Working Party and Council Working Groups).
    - Possible entry point of contact for external parties relevant for the CSIRTs Network (see item: International Contacts).

ENISA

- ENISA will provide the Secretariat for the CSIRTs Network.
- ENISA will provide a supporting role to the work of the Chair and the whole functioning of the CSIRTs Network.
- ENISA will, at the request of the Chair, organise the meetings of the full CSIRTs

Network and working groups, provide technical support for any teleconference discussions and provide minutes of the meetings and discussions.
- ENISA will support the work of the rotating Chair trio and will provide continuity between the trios. This will include assisting with drawing up priorities, aims and policies, including those related to further forms of operational cooperation, as requested by the Troika.
- Basic communications for the CSIRTs Network will be managed by ENISA. Initially this will be done via email and ENISA will be responsible for ensuring that all CSIRTs are invited to the communications.
- ENISA Supports the Chair trio in drawing up the guidelines on operational practices and any other guidelines, standard procedures that the network will wish to develop.
- CSIRTs Network Members are responsible for coordination in case of an incident or crisis, on request, ENISA may provide active support.

Working method and trust building
- The CSIRTs Network should meet at least twice a year and work mainly on a remote basis. If necessary, this could be complemented with additional meetings and teleconferences. Preferably, meetings should be planned around conferences at EU level and other relevant CSIRT meetings.
- Trust building sessions are to be maintained throughout the lifetime of the CSIRTs Network, in particular during the initial phase.
- Regarding trust building measures in communities, participating CSIRTs could use existing methods or look into researched methods[5].
- English will be the working language of the CSIRTs Network.

Expert group
- The CSIRTs Network should allow setting up expert groups on specific issues open to nominated CSIRTs Network Members and which results should benefit to the CSIRTs Network as a whole.
- The task of the groups will include, but not limited to, developing solutions and technical recommendations in specific areas.
- Expert groups should be reflected in the action plan and the results should be shared with all CSIRTs Network members.

Guests
In case decided by its members, the CSIRTs Network may decide by consensus to invite guests (non-EU countries, international organisations, private sector representatives) to specific meeting and/or specific agenda items. Invitation of guests should be motivated and guests should be invited on a strict ad hoc basis. Only EFTA countries may be invited permanently as guests.

Implementation roadmap for the tasks provided by article 12.3
Relevant elements of the ENISA Work Programme in the CSIRT area should be referenced in these tasks.

Report
In line with the NIS Directive[6], the Chair trio draft a report to the Cooperation Group once every 18 months, with assistance of the Secretariat, if requested. Afterwards it should be discussed and coordinated in the CSIRTs Network. This discussion should be reflected as such in the report and finally be presented there and submitted to the Cooperation Group.

[5] Such as the papers issued by ENISA “Scalable and Accepted Methods for Trust Building in Operational Communities" and "Good Practice Guide Network Security Information Exchanges"
[6] Article 12.4 of the Network- and Information Security Directive

Review of Terms of Reference and Rules of Procedure
Every 18 months the CSIRTs Network will review its Terms of Reference and Rules of Procedure and adapt or amend these on a consensus-basis when deemed necessary.