Minutes of National Laison Officer's Meeting, February 2014

Draft 20 March 2014

Document History

//DRAFT ONLY - DELETE THIS SECTION AND PAGE UPON FINAL PUBLICATION

Date	Version	Modification	Author
20.03.2014	1.0		KC

1 Opening by Chair, presentation of ENISA's Strategy and 2015 work programme, feedback on dissemination forms

Steve Purser, ENISA

Chair of the meeting, Steve Purser, Head of the ENISA's Core Operations department, welcomed the participants.

He then gave an introduction on the Agency's new mandate and presented ENISA's strategy and 2015 work programme. The planning framework is more restricted, plus core priorities are replaced by key areas. ENISA is moving towards a multiannual thematic area approach.

Strategic objectives have been broken down into core priorities. The core priorities are the same as the 'key areas' in previous versions of the strategy document.

Each core priority has been assigned to the relevant strategic objective.

ENISA's strategic objectives are:

1. To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network & Information Security (NIS).
2. To assist the Member States and the Commission in enhancing capacity building throughout the EU.
3. To assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security.
4. To enhance cooperation both between the Member States of the EU and between related NIS communities.

The opening session was concluded by giving specific mention to the spreadsheets sent to Member States (MS) on 11 February 2014, to answer the MS request on systematic information exchange with regards to deliverables. MS can use them as an organizational tool with regards to dissemination of deliverables. However, MS cannot be involved in the planning and running of projects.

There will be a single contact point at ENISA, Katerina Christaki who will then forward the request to the project managers concerned. Any mailshot/communication from ENISA to the NLO network is send by the NLO Project Managers (KC and SG). ENISA experts may contact and follow up on these contacts with member(s) of the NLO network for issues related to their projects provided that the NLO network PMs (KC and SG) are always in copy.

NLOs even though not a structural entity, constitute a valuable network of ENISA. Feedback from and towards the network has been improved but further work needs to be done towards this direction.

2 ENISA NLO activities update

Katerina Christaki, ENISA

Katerina Christaki, ENISA's project manager for the NLO network since October 2013, gave an update on ongoing activities, plus the role of NLOs. NLOs main task regards dissemination of ENISA's activities and products, plus Community building.

More specifically:

Community building:

- NLOs maintain and grow a contact list or mailing list of relevant experts in NIS.
- Besides a mailinglist social media networks (Linkedin, Twitter) could also be used.

Dissemination/information:

- ENISA keeps NLOs informed about activities, news, etc.
- Periodically (every 2-3 months) NLOs should send an update about ENISA's activities to the local community.

Surveys:

- For specific projects ENISA may run surveys to NLOs
- NLOs forward the survey to the local community.

Calls for participation:

- For specific projects may want to involve experts and send a call for participation in expert groups.
- NLOs forward these calls to the local community

Ideally NLOs should gather feedback from local communities on ENISA's work program and collect ideas about ongoing NIS issues. Periodically ENISA would collect this feedback and send it to the PSG and MB for consideration.

2.1 Feedback on additional communication channels

Responding to the question whether information on the ENISA-NLOs collaboration should remain public, or stored in a private communication channel, NLOs to their great majority agreed that information should remain public. FR, DE and EE noted that there is information concerning the internal procedures and work in progress that cannot be revealed to the public.

The *Chair* noted that NLOs that disagree with putting information on the public website would need to define which type of information needs to remain private.

ENISA will examine the possibility of creating a central repository that NLOs could use to deposit information in Q2 2014.

SK stated the need to translate ENISA deliverables in local languages. A great part of local communities does not speak English and this is the main obstacle to dissemination.

Manuel Silvoso from LU gave a presentation on the status quo of NIS in his country.

During the morning session the Greek NLO announced an event of the Greek Presidency (www.gr2014.eu) taking place 6-7 March, 2014 in Athens, GR and asked for dissemination of the event through the network.

---

3 ENISA threat landscape report

Louis Marinos, ENISA

The ENISA threat andscape(ETL) is a collection of top cyber-threats that have been assessed in the reporting period, ie. end 2012-end 2013. In addition to an overview of current cyber-threats, the ENISA threat landscape delivers predictions for threat trends regarding emerging technology areas.

The objective of this work is to provide stakeholders with information about developments in the cyber-threat landscape and to identify threat trends for the near future, ie in the coming year. For the prediction of trends, important areas of IT innovation and development were taken as a basis. The assessed top threats from 2013 are mapped to these areas and thus an emerging threat landscape was created.

The report is based on a comprehensive information collection of publicly available open source material. Reports appearing after this period will be considered in the next year's ETL, to be delivered around the same period in 2014.

FR and NL found the report very interesting. FR suggested to track the usability of the presentations such as this one.

4 Security measures for smart grids

Konstantinos Moulinos, ENISA

ENISA's work on smart grids cybersecurity identifies a set of minimal measures needed for security and resilience. The European Commission has decided to task ENISA with the organisation of consultations on these minimum security requirements with national cyber security authorities and the Energy and ICT industry, and possibly also selected non-EU partners.

The presentation aimed at introducing ENISA's smart grid cyber security project to the NLOs and inviting them to actively participate in the Agency's activities in this area for 2014.

NLOs asked for an early notification for the relevant activities which their participation is needed.

5 ENISA supporting the National Cyber Security Strategies

Dimitra Liveri, ENISA

In this session, Dimitra Liveri presented the activities on two topics: cloud security and cybersecurity strategies. On the Cloud activities she gave an overview of the past publications, the collaboration with the EC in the implementation of the EU Cloud strategy and the 2014 activities. She also presented the ENISA Cloud Security and resilience experts group, focusing on the "governmental

cloud" representatives and how the NLO network can assist ENISA in engaging more experts in this year's studies.
On the topic of national cyber security strategies, the past work and publications on the topic as well as the future objectives were presented. ENISA has setup an experts' group on national cybersecurity strategies to support the MS adopting and evaluating a cybersecurity strategy.

A separate request will be sent to the NLO community on the specific topic. (Completed)

A call for Cloud security project will be announced end of Q2.

6 EU legislation

Christoffer Karsberg, ENISA

Christoffer Karsberg presented ENISA' s work on Implementing EU Regulation. In Art 13a of the Framework Directive in the Telecom Reform, ENISA is supporting the National Regulatory Authorities (NRAs) implementing the Directive on a national level.

ENISA chairs an expert group with the NRAs and together the group drafts guidelines for the NRAs on security measures and incident reporting. Also the procedures for annual reporting from the NRAs to ENISA and the European Commission are agreed upon. Annually ENISA produces an aggregated summary from the reported incidents, showing patterns and trends in incident across the EU. Then Mr. Karsberg explained the benefits in identifying synergies between Art 13a and Art 4 in the ePrivacy Directive, especially regarding security measures and incident reporting. Regarding Art 15 of eIDAS, ENISA is preparing to set up an expert group of competent national authorities to start the work on the scope for incident reporting, given that the regulation is approved. Also the Electronic Communications Reference Group and the upcoming Infrastructure Security and Resilience Reference Group were presented.

Mr. Karsberg especially invited the NLOs to promote these two groups to their national constituencies.

NL proposed to create a kernel of people to find synergies between Art13a and Art4, in order to save resources.
FR asked if the membership in the presented expert groups was fixed, or if other entities can join. ENISA replied that the Art 13a Expert Group is for NRAs, for entities that are concerned by the regulation. The Electronic Communications Reference Group is for CISO experts at Telecom operators and ISPs and the Infrastructure Security and Resilience Reference Group is for experts from the internet infrastructure community and relevant public bodies.

ENISA will send a request to NLOs for support in setting up the expert groups and engage competent authorities.

7 ECSM 2014

Daria Catalui, ENISA

Daria Catalui presented the European Cyber Security Month's planning for 2014. ECSM 2014 is a project of all Member States and not just ENISA's, as it focuses on creating awareness on NIS issues. The single point of information for this project is the website www.cybersecuritymonth.eu, or the community developed on Twitter, @CyberSecMonth.

NLOs were invited to support ECSM 2014 by acting as the general contact point for their country, to network between representatives at country level with the help of EC representations and support ENISA in mapping stakeholders with a priority for universities of all disciplines.

Steve Purser, added that in the near future the cybersecurity challenge will take place, a hacking competition targeting universities ofa broad curriculum.

8 Supporting and developing CERT capabilities for financial sector

Andrea Dufkova, ENISA

Andrea Dufkova gave an introduction on CERTs and then presented the European Financial ISAC (FI-ISAC) initiative whose members are:

- Banks, national CERTs and Law Enforcement Agencies
- ENISA, Europol, ECB, EPC and the EC and
- Financial operators

The purpose of this initiative is information exchange on:

- Vulnerabilities, technology trends and threats
- Incidents
- ICT related subjects

FI- ISAC holds two meetings a year. The meeting details cannot be googled. The information exchange in the group follows a protocol according to degree of confidentiality. There are maximum three participants per country. Their next meeting will be held in Athens, Greece on 28-29 of April 2014 and will be hosted by ENISA.

NLOs are kindly requested to inform their national networks about EU FI-ISAC and suggest participation.

9 Cyber Europe 2014 (CE2014)

Panagiotis Trimitzios, ENISA

Panagiotis Trimitzios presented ENISA's work on cyber-crisis cooperation through the coordination of pan European and International exercises. He spoke more specifically on the current exercise CE2014 and it's implementation.
CE2014 focuses on the escalation and aspects not covered in the past years. This year the exercise will be implemented in three phases happening at different points in time, technical (TLEx),

operational(OLEx), and strategic (SLEx). In TLEx mostly members of technical teams play (technical-level), in OLEx mostly the leaders/managers of these teams play (operational/tactical level), while SLEx refers to high level politicians.

All EU and EEA MS participate this year, a total of 29 countries apart from LT,MT and LI.

Austria will amend CE2014's scenario and use it at its national cybersecurity exercise.

To answer PL's question on how the escalation aspect can be checked since the exercise is split into phases, Mr. Trimitzios answered that this is the only feasible way to do it, otherwise the complexity of the exercise would increase exponentially.

10 Dan Tofan: ACDC project

Dan Tofan, NLO Romania

Fourteen (14) countries are part of the ACDC (the Advanced Cyber Defence Center).

ACDC is a European funded project. The goal of the project is to provide the security tools and services to fight against botnets in Europe.

In order for MS to participate, they need to send a letter of interest to ACDC management.

The afternoon session was concluded by Luukas Christian Ilves (EE NLO) giving an update on the current NIS situation of Estonia and Viktors Lipenits (NLO LV) reported on the latest developments in Latvia.

11 Round table

The actions summing up the round table discussion, that took place by the end of the meeting, are the following:

1. NLOs to include a link to the ENISA website in their respective organisations websites after conference.

2. Spreadsheets should be used by NLOs as a tool to organise the dissemination of ENISA deliverables. It is a tool that will be further developed in order to give insight to both sides on priorities regarding projects. ENISA will send a relevant communication in Q2 for gathering feedback on these forms.

3. NLOs are requested to reach out in their countries for a suitable candidate to join the EU FI-ISAC initiative. A law enforcement representative is needed at this stage(police, cybercrime units, operational personnel..). For providing input, or for any enquiries please contact Cert-relations@enisa.europa.eu . (ongoing)

4. NLOs were invited to support ECSM 2014 by acting as the general contact point for their country, to network between representatives at country level with the help of EC

representations and support ENISA in mapping stakeholders with a priority for universities of all disciplines. (ongoing)

5. NLOs should appoint an expert for smart grid security in their country. A communication will be sent out by ENISA with regards to this.(ongoing)

6. NLOs are invited to promote the Electronic Communications Reference Group and the upcoming Infrastructure Security and Resilience Reference Group, to their national constituencies. ENISA will send a request to NLOs for support in setting up the expert groups and engage competent authorities.(ongoing)

7. NLOs are requested to provide contact points in the area of NCSS (national cybersecurity strategies). ENISA will make a formal request to the network.(completed)

8. ENISA should provide a set of slides that could be used by NLOs to 'market' the Agency. (ongoing)

9. ENISA will investigate the possibility to put more structure in the work NLOs have to do (suggestion from RO).

10. ENISA should set up a web interface serving as a repository that will help in the coordination of NLO activities. This web interface will be containing a group of folders that NLOs could use a central repository of information. Prior to this, ENISA will investigate with NLOs the type of information that will be included in this interface. Time of implementation Q2/Q3 2014.

11. ENISA/NLOs will check whether the proposal of Luukas Christian Ilves (EE) to have a group of NLOs taking the lead of the NLO Community, is feasible. (open)