www.enisa.europa.eu

Interview ”Good Practice Guide Network Security Information Exchanges”

Dr. Evangelos OUZOUNIS
Senior Expert
Network Security Policies
Technical Competence Department

Dr. Konstantinos MOULINOS
Seconded National Expert
Network Security Policies,
Technical Competence Department

Interview with Evangelos Ouzounis and Konstantinos Moulinos, Senior and Seconded National Experts respectively - IT Security Policies Technical Department. ENISA has recently launched a good practice guide to assist Member States and other relevant stakeholders in setting up and running Network Security Information Exchanges in their own countries.

First of all, what was the reason for ENISA to produce this good practice guide?
As from January 2008, ENISA has launched its programme on resilience of communication networks. It is divided in three areas namely policies and regulations, providers' measures and technologies. This guide is part of this programme. In the area of policies and regulations ENISA took stock of the Member States' activities and one of the questions then was about information sharing. We found out that only a few Member States were deploying these mechanisms, which is the reason for coming up with this good-practice guide that we are now hoping that other Member States will implement as well.

What are the countries that have developed such NSIEs and are to work as good examples for other Member States?
The United Kingdom, the Netherlands, the Scandinavian countries, Switzerland, and a few others have already developed a systematic way to information sharing. This effectively means public private co-operation on vulnerabilities, threats and good practices.

What would you say is the main reason that so many Member States still haven't developed a way to discuss this?

One of the reasons is that many of the countries are not very well advanced in the area of network and information security. They don't have the appropriate regulatory and/or policy environment, and they lack a number of elements that is required to deal with these topics. In addition another problem is the lack of experience in working together both the public and the private sector. The third issue is that some countries practically are not aware of these mechanisms. Instead they first focus on regulatory measures than developing partnerships with private sector.

There are differences in the Member States level of awareness and knowledge in this area. However countries, which still haven't developed an NSIE, are now requesting something concrete to work from. The proposed good-practice guide is a first and hopefully the right step towards this direction. .

Is it a problem for private and public stakeholders to cooperate?
There are several problems or obstacles identified in the area of information sharing and this is one of the issues that we have to explore further. ENISA intends to make a study in the coming year, in order to explore barriers and obstacles to information sharing with regard to NIS (Network Information Security). However, there are several identified obstacles listed in the report. It is true that working together with the private sector, which is the main owner of the critical information infrastructure, needs to be done in a way so that trust develops among the members of this group. It is necessary to follow a soft regulatory approach and develop trust over time.

There are other issues like for instance how to handle the sharing of information of competitive nature. Sometimes it is a matter of rules and regulations prohibiting information to be shared from one partner to another in these partnerships. Another important issue is the confidentiality of the information exchanged between, especially the public, partners.

Furthermore the participation of regulators or law enforcement is an issue to consider when shaping the NSIE. Every country has its own answers or approach to this. The good practice guide raises issues like these and provides the reader with alternatives for consideration.

So what is your advice on how to tackle these co-operation issues?
The trust among the members of all initiatives and a platform like this are key success factors. Without trust there is no way to share information. It takes time to change the stakeholders' mentality and their perceptions, but the NSIEs have proven to be very useful to this end.

The stakeholders must be able to discuss the problems they are facing in an open and transparent manner and in that way create trust among each others

Normally the amount of information shared between the stakeholders increases after a couple of years, when they have gotten to know each other better. The private stakeholders might, in the beginning, be afraid of talking about some problems if they think that this can lead to the public authorities imposing new regulatory interventions. Another issue for the private stakeholders is that they are afraid that the competitors might use the information shared.

It seems like the different approaches varies in the Member States. How is the good practice guide then best used?
For the best use of this good-practice guide it is important to be aware of the roles of the own country's competent authorities. The guide includes examples on how several Member States implemented this concept. When there is momentum on an issue, the guide just presents the good practice. If there are different, equally important, approaches then the guide just presents them without taking position on the merit of them.

What is your main advice on why those Member States who haven't yet developed an NSIE platform should do so?
It is necessary to have these platforms in place in order to understand an environment that changes rapidly. If you want to develop a holistic view of the threat environment and the risks in telecommunication network services and applications you have to collaborate with the private sector. Furthermore, you need a joint understanding of the problems. It is better to work together to find solutions and share information instead of imposing new regulations.

The report focuses on national, as well as pan-European platform. When will this pan-European platform be in place?
Basically the strategic objective with this guide was to help member states develop their national information sharing capabilities. However, all these countries are dealing with similar problems and by bringing them together, the understanding, knowledge and the analysis of these topics might improve. We hope that this is going to be the scenario, i.e. national NSIEs cooperating, but we are aware that this might take a few years. The idea is not to replace the national NSIEs but rather to improve them through constant dialogue with its other.

Aren't the Member States already exchanging information regarding NIS?
Some Member States are, but these co-operations are not yet official platforms. The first priority right now is to increase the number of Member States that have an NSIE. The second priority is to investigate the possibility of a pan-European platform.

What will ENISA's role be in this pan-European platform?

ENISA's role is to facilitate and be the catalyst for a pan-European platform. ENISA has been invited to play a coordinating role between Member States to facilitate the exchange of information and good practices.

Who is usually initiating a Member State's NSIE program and what are the costs involved with such a program?
This varies between the Member States. Usually it is the governments' responsibility to initiate this in terms of logistics, financing and planning, but it also depends on the reaction from the private sector. For example in the UK you could say that the private sector is the initiator, but in the Netherlands it started as a governmental activity but then other agencies joined.
When it comes to the financing of an NSIE program it is not a big cost. Normally it is a matter of four to six meetings per year and the only costs involved are logistics (e.g. venue costs, food, etc.). In other words, it is a matter of persuading the different stakeholders to participate in a program like this, rather than a problem related to costs.

What is ENISA doing now to spread the information about NSIEs?
We will now be arranging a number of workshops with different stakeholders, where we will try to bring them together and get them to understand the benefits of NSIE platforms. The guide will be explained in detail and we will also explain how the Member States can implement it in reality.
Two other good-practice guides on incident reporting mechanisms and national exercises will also be presented during a workshop in Brussels and discussed during a major conference organised by the Swedish EU Presidency in Stockholm in November.

For full report:
http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/good-practice-guide

More information on the Resilience Program:
http://www.enisa.europa.eu/act/res

For further details, contact:
Dr. Vangelis OUZOUNIS, ENISA Senior Expert - IT Security Policies
Technical Department, Evangelos.Ouzounis@enisa.europa.eu
Ulf Bergstrom, Press & Communications Officer ENISA,
press@enisa.europa.eu, Mobile: +30 6948 460143