Interview with Jeremy Beale, Head of ENISA’s Stakeholder Relations Unit on the recently launched ENISA “Country Reports”.

Could you tell us about the improvements in this report compared to the first country reports?
We have done some restructuring in this report compared to the previous ones to make them a bit less general about countries. We have tried to focus more specifically on network and information security and ENISA’s priority issues in this area, which is what we assume the target audience is really interested in. The first reports also had a significant overlap with the Who-is-Who Directory, which has now been cut down. However, you can still see who the responsible organisations are and the links between them.

Will we see this report every year?
We are not producing the reports just for the sake of it, but as long as EU Member States and stakeholder communities find it useful we will. We are also looking at having the Who-is-Who Directory and perhaps the Country Reports solely online from now on.

Are the readers interested in what is being said about their own country?
We don’t currently have many means for precisely assessing what the readers are the most interested in, but our expectation is the other way around – that readers use the reports to find out what is going on in other countries that may be of use to them domestically. This explains the manner in which the reports are produced, i.e. giving readers detailed information on what is being done in the specific areas identified by Member States and the Commission as crucial to ENISA’s Work Programme. But it would be easier to assess what readers are most interested in when we have html-based versions where we can track fully what people are actually looking at.

Could you just briefly explain what the Who-is-Who Directory is?
Basically, it is a directory for readers to turn to when they see something being done in other Member States, such as good practices that could be useful to them, and want to get in contact with those involved. A lot of the problems in network and information security - or NIS - simply arise from people not knowing who to contact or how to find relevant organisations.

Is the Who-is-Who Directory being updated regularly?
The paper version is produced only once a year. But we now have the directory entirely online so we can update this regularly as we are informed of changes by our Member State and stakeholder contacts.

In the report you mention that it is not intended to provide a separate analysis, or to perform benchmarking or ranking of the NIS specific elements of these countries. Is there a reason for this, or is it just not possible?
There are three basic reasons for this. First of all, since practices are still new and not standard across the EU, making comparisons is somewhat meaningless. Second, it is also difficult to say at this point what should be compared, since policies, data collection etc. in the Member States vary a lot according to their differing historical economic, social and security concerns and needs. However, this year's report has a more comparative methodology, since we are looking at the same things in all of the Member States. Third, it is not in ENISA's remit to benchmark EU Member States.

In general, it is noted that many information security incidents are reported and handled via national/governmental CERTs. Would you say that the CERTs are the most important thing to have in NIS?
CERTs are a vital element of what countries need to have in place. They are organised groupings of people in important places that can help identify what is going on in terms of NIS and develop appropriate responses. However, they are not sufficient for a Member State if it is to be properly prepared to deal with the range of threats and incidents that can or will occur.

Has the geographical distribution of the CERTs evened out?
CERTs have often grown organically in sectors like academia, oil and banking; and historically CERTs have also been growing in high value sectors with a lot of online activity. What is newer is the growth of national or governmental CERTs. In the UK for example, they have a CERT just for the government, and they also have lots of private sector CERTs. But there is no national CERT for the whole country. In some countries, particularly in the newer Member States, there have not been many private or national/government CERTs at all. Over the last few years, ENISA has helped to establish national or government CERTs in these countries, which is now almost complete.

Germany, the United Kingdom, followed by the Netherlands show very high interest and activity related to CERTs. What does it take for the new Member States to come up to the same level of CERT activity?
ENISA has been working on transferring technical capabilities to these latter Member States. This enables them to establish national government CERTs, which can then help in establishing private sector CERTs. The private sector does, to a certain extent, already have CERTs in sectors where there are major foreign investors in newer Member States, such as banking or telecommunications,

and this can make the job easier in terms of having private sector partners whom we can work with.

In terms of secondary legislation, the overall situation is very different from one country to another. Why is this?
It is a historical legacy to a large extent. Network and information security has traditionally been viewed from a national security and/or law enforcement perspective, where concerns and competences have differed quite a bit between countries. National characteristics are often a starting point also for the civilian development of NIS capabilities. We are still in the early days of developing NIS capabilities outside a traditional national security or law enforcement context.

Are there some inspirational examples you would like to highlight?
I would be reluctant to highlight any one particular example, and things are moving so fast and ENISA is still learning a lot itself. One of the things we do point to is the value of a comprehensive or overall framework for network and information security for countries.

Risk Management and Emerging NIS Risks – in the report you mention that the national risk management process in countries varies, but could you say anything about specific countries (such as Norway) or the national risk management process in general?
In some countries there is no risk management process in place at a national level, while in others there is either a formal risk management process in place or several specific activities are undertaken to address the topic at a national level (e.g. the case of Norway). Risk assessment of emerging and future risks again isn't the same in every country. It can, for instance, be linked to the national research and development strategies of Member States.

There are several inspirational cases. But would you say that network resilience aspects have grown more important?
Network resilience has certainly gained a higher political profile recently. Over the last year or so the European Commission has issued a communication on this, the Council of Ministers has made a number of statements on the importance of resilience etc. One example that you could say sparked this off was the attacks on Estonia, and another was a couple of years ago when an unusual amount of snow in the UK meant that important websites were impaired or went down because of unanticipated surges in demand. The growing importance of the internet and of mobile data demand makes the necessity of network resilience increasingly clear.

Apart from the Country Reports, what is being done in terms of looking at NIS?
The Country Reports are valuable contributions to identifying what's going on and there are also various publications provided by commercial security organisations. There is also work being done in the OECD looking at what is happening internationally. Countries themselves are starting to boost their domestic coverage of the issues, and the European Commission is focusing on policy making and coordination, trying to identify what needs to be done on a European and international level.

What are ENISA's conclusions?

One conclusion is that we are still in the early days of understanding the importance of this to us and what we need to learn. It is important to have a national CERT or an extensive development of CERT capabilities in your economy as a part of a broader cyber security strategy. The CERTs are important building blocks, but insufficient on their own. When it comes to network resilience it is important to know who is doing what in the case of a breakdown. Another thing is that it is now well understood is that good cooperation between the public and private sectors is essential.

For report:
http://www.enisa.europa.eu/act/sr/country-reports

For press release:
http://www.enisa.europa.eu/media/press-releases/eu-agency-maps-key-online-security-actors-strategies-good-practices-in-europe

For further details contact:
Jeremy Beale, Head of ENISA's Stakeholder Relations Unit, Jeremy.Beale@enisa.europa.eu
Ulf Bergstrom, Spokesman ENISA, press@enisa.europa.eu, Mobile: +30 6948 460143