Q&A

CYBER EUROPE 2012

Q: Why conduct pan-European cyber exercises?

A: As cyber crises occur on larger scales, and grow more transnational in origin and effect, managing them effectively requires international cooperation. The world is ever more connected (by online networks and services) and therefore international cyber cooperation is required to support and protect the information society we live in.

Cyber exercises are an important tool to enhance, improve and focus on large scale cyber crisis cooperation. Supporting EU-wide cyber security preparedness exercises is one of the main actions of the Digital Agenda for Europe of the European Commission. Strengthening Europe's cyber defence and combating potential online threats to essential infrastructure helps ensure that businesses and citizens feel safe and secure online. Moreover, making the best possible use of ICT could help speed up economic recovery and could lay the necessary foundations for a sustainable digital future.

Q: When did the first pan-European cyber exercise take place?

A: The first pan-European cyber exercise (Cyber Europe 2010) was conducted on 4th of November 2010.

Q: What was the objective of Cyber Europe 2010?

A: The objective of the exercise was to trigger communication and collaboration between countries in Europe to try to respond to large-scale attacks.

Q: What were the main recommendations and lessons-learned from Cyber Europe 2010?

A: The findings and recommendations of the participating EU Member States indicated that Cyber Europe 2010 was a useful 'cyber stress test' for public bodies in Europe. One of the main recommendations drawn from CE 2010 was that the private sector could add value in future exercises.

Another finding was that Member States should be well organised internally, e.g. by developing national contingency plans, which are maintained and tested on a regular basis through national exercises.

Q: How is Cyber Europe 2012 different from Cyber Europe 2010?

A: Cyber Europe 2012 is a more extensive, more sophisticated exercise that is based on experience and recommendations from Cyber Europe 2010. CE 2012 has more ambitious objectives. Following one of the main recommendations of CE 2010, the private sector is participating in Cyber Europe 2012.

Q: What are the objectives of Cyber Europe 2012?

A: The objectives of Cyber Europe 2012 are:

1. Test effectiveness and scalability of existing mechanisms, procedures and information flow for public authorities' cooperation in Europe in case of large scale cyber incidents;
2. Explore engagement and cooperation between public and private stakeholders in Europe in case of large scale cyber incidents;
3. Identify gaps and challenges on how large scale cyber incidents could be handled more effectively in Europe.

In addition:

- This exercise will help test the way that the exercise was planned, organised and conducted in order to identify any deficiencies. This way future cyber exercises can make use of the lessons learned and improve their planning and organisational quality.

Q: Who is participating in this exercise?

A: All EU/EFTA MS participate in the exercise in one way or another. In addition, this is the first time both public and private sector stakeholders are participating together in a pan-European exercise.

Q: Will there be a repeat of this exercise in the future?

A: It is ENISA's aim that further exercises will take place in the future. It is the intention that Cyber Europe exercises are conducted every two years. Cyber crisis cooperation and response in Europe are maturing. These exercises are very effective tests of our systems and preparedness, and provide invaluable feedback for making improvements.

Q: How is the exercise planned?

A: Cyber Europe 2012 is organised by an EU planning team which consists of representatives from the participating countries. ENISA facilitated various workshops, teleconferences, and training events to support the process. Planning team members also formed a number of special "taskforces". Each taskforce was responsible for a specific part of the planning and preparation of the exercise.

Q: What are the next steps?

A: Work will continue in this area. Large-scale cyber incidents are rare, so exercises are essential as a way of being able to be ready if a real crisis occurs. Experience from exercises forms the basis for further preparation – particularly in the development of operational plans and making sure sufficient people and resources are available. The exercises take place as part of a "lifecycle" – plans developed from lessons learnt in exercises are themselves tested in future exercises. The aim is to ensure that, in the event of an actual crisis, the operational "routines" are in place that ensure the optimal effective response.