EU-US joint CIIP Exercise, Cyber Atlantic 2011 – Raznan Gavrila

Speaker: Raznan Gavrila is the Network and Information Security Operation Officer, CIIP & Resilience Unit, at European Network and Information Security Agency (ENISA).

The European Union's cyber security agency, ENISA[1], organised an EU – US Joint CIIP exercise, called Cyber Atlantic 2011, which was held on 3rd November 2011. The idea for this exercise was discussed during a number of events and initiatives including: EU-US summit of 20 November 2010 (Lisbon); EU-US Working Group on Cybersecurity and Cyber Crime (EU-US WG). The holding of the event was formally announced on 15th April 2011 during the Hungary Ministerial Conference by Commissioner and DHS Secretary and ultimately held on 3rd November 2011.

Cyber Atlantic 2011 was the first joint EU-US cyber exercise and was comprised as a centralised table-top exercise in which over 20 countries were involved (17 countries played). The overall planning and preparation was carried out by ENISA and DHS incorporating facilitation and overall management of the preparation and evaluation phases. The planners teams were from: AT, BE, EE, ES, FI, FR, HU, IT, NL, RO, SE, UK, ENISA, US/DHS, EC, JRC.

Cyber Atlantic 2011 was an exercise of an exploratory nature with the following objectives:

- Explore and identify issues in order to improve the way in which EU Member states would engage the US during cyber crisis management activities;
- Explore and identify issues in order to improve the way in which the US would engage the EU Member states during their cyber crisis management activities, using the appropriate US procedures;
- Exchange good practices on the respective approaches to international cooperation in the event of cyber crises, as a first step towards effective collaboration.

There was a two part scenario: Advanced Persistent Threat (APT) scenario with a hacker group, "Infamous" exfiltrated sensitive documents from EU and US – 'Euroleaks' web site and Supervisory Control and Data Acquisition (SCADA) scenario highlighting vulnerabilities leading to backdoors (and failures) on Programmable Logic Controllers of power generation equipment.

The lessons learned (tentative) from Cyber Atlantic 2011 were:

- Mechanisms/structures for cross-border cooperation do exist; however, each country needs awareness of all communications options ;
- Exchange Standard Operation Procedures (SOPs), trainings, exercises;
- Exercises need increased participation from all three: Technical, Law Enforcement, Policy/Political;
- Single Point of Contact in EU for US would help but is not compulsory;
- More exercises/workshops are needed!

[1] http://www.enisa.europa.eu/