

Protecting European Critical Information Infrastructures

Essay by Daniele Catteddu, Risk Management Expert, European Network and Information Security Agency (ENISA)

The increasing attention to information and communication technologies (ICT) as a fundamental engine for our society is highlighted in a number of recent strategy documents (i.e. i2010, Digital Agenda, Commission's Communication on Critical Information Infrastructure Protection (CIIP)) in which new and concrete policy and regulatory provisions for the improvement of the security and resiliency of public e-Communications are proposed.

ENISA, the European Network and Information Security Agency, in its advisory role to the EC and MSs fully recognizes the challenge of achieving higher level security and resilience for communication network and service launched, in 2008, a medium term set of actions, under the name of "CIIP and Resilience Program". Its objective is to improve the preparedness of the public and private organisations in preventing and reacting to security incidents and faults.

To reach this ambitious goal, ENISA is facilitating the exchange of information between EU institutions, the public sector and the private sector, preparing and disseminating good practices, providing guidelines and suggesting appropriate technical and organizational security measures. The driving principles behind all ENISA actions and proposal are transparency, cooperation, collaboration, consistency and harmonization.

ENISA's CIIP and Resilience program consists of a number of projects that started in 2008 with a stock taking and analysis of Member States' (MS) policy, regulatory and operational environments related to the resilience of public eCommunications Networks, and a comprehensive analysis of provider measures.

In 2009 ENISA implemented this recommendation by developing three good practice guides on information sharing, incident reporting mechanisms, and resilience exercises.

This year, the Agency is focusing its efforts on supporting Member States in the implementation of Art.13 a of the newly adopted Telco Package, organizing a Pan European Exercise and producing studies in the areas of botnets, metrics for resilience, networks interconnections and trusted information sharing systems.

Implementing Article 13 a

Article 13a of the new Framework Directive calls on Member States to ensure that providers of communication services take appropriate measures to manage the risks posed to the security of their networks and services and to notify the competent national regulatory authority of a breach of security that has had a significant impact on the operation of networks and services. Article 13 a introduce also an annual reporting from NRAs to ENISA.

In the context of implementing Art.13, ENISA is acting as a facilitator, engaging the competent regulatory authorities in each Member State in a structured dialogue on the key points of ie, incident reporting (eg, conditions, parameters, and impact),

minimum requirements for security and resilience, and on how incidents should be reported to ENISA on an annual basis.

The main objectives of ENISA, as regards the reporting of security incidents and the implementation of article 13a, are to:

- define a unified scheme for incident reporting to ENISA and the European Commission that delivers added value to the Member States;
- work together with Member States and the private sector to increase their level of preparedness by developing minimum security requirements for addressing risks to resilience and security;
- assist Member States in developing a common understanding of the main issues of article 13a and thus avoid fragmentation across Member States;
- identify, disseminate and consolidate the use of good practices in the area of incident collection and reporting;
- support the creation of a trusted environment or community for information sharing between Member States.

ENISA will continue in this effort until all the 27 Member States have completed the implementation in order to make possible an harmonized implementation of the directive.

Botnets

Current estimates of the extent of infected machines and botnet activities vary wildly. For example, in the analysis of the takeover by the Torpig botnet, researchers found that the relation between the number of unique infected hosts and IP addresses was about 1:7, based on an analysis of unique botnet identifiers. Yet most figures are based on the number of IP addresses on which bots are detected.

The objective of ENISA's study on botnets is to come up with a map of methodologies for the detection, measurement, defence and disinfection of botnets, as well as a comparative evaluation of these methodologies, and a recommended set of best practices.

ENISA also aims to stimulate an ongoing collaboration between the various groups involved in combating botnets and longer term information sharing, to support targeting more efficient use of the limited funds available for fighting botnets.

Currently ENISA is evaluating various strategies for measuring botnets and their effectiveness and is looking at:

- Technical issues – how best to discover and disinfect botnets, and, just as important, take down the botnet herders' command and control centres.
- Legal issues – some defensive measures which might be effective are not practical because of legal obstacles. Either they are illegal or they take too long because of red tape.
- Economic issues – botnets only exist because they make money for their owners. How can we find ways of 'cutting off the food supply'? Another important issue is the problem that some organisations tend to lose reputation and revenue if they inform users of botnet infections, even

though they are not responsible.

- Policy initiatives – what kinds of policies are effective in reducing the number of infections? For example, how effective are so-called walled gardens – where ISPs redirect infected machines to a safe online environment where they are provided with guidance on how to disinfect their machines.

The final report "Botnets: detection, measurement, disinfection and defence" will be published in Q4 2010.

Pan European Exercise - CYBER EUROPE 2010

Cyber Security 2010 is the first pan European Exercise on Critical Information Infrastructure Protection (CIIP). It is organised by the EU and EFTA Member States, managed and facilitated by ENISA supported by the Joint Research Centre (JRC) of the European Commission.

There 30 countries involved by taking part in the planning Workshops and decisions, while 22 of them will be actually playing.

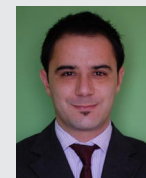
The exercise scenario concerns incidents that involve the resilience of the Internet, and it will focus in particular on the cross-country contacts and communication procedures in case of a large scale cyber incident. The objectives of the exercise include:

- building trust
- increase the understanding on how cyber incidents are handled
- test communication points and procedures between participating MS
- understand interdependencies between key actors within each MS
- promote mutual support between MS

The results of the exercise will be made public in early 2011.

Daniele Catteddu

Risk Management Expert, European Network and Information Security Agency (ENISA)



Daniele Catteddu works at ENISA (European Network and Information Security Agency), where he is responsible for supporting EU Member States in implementing ENISA's obligations in the

new European Telco Package. He has also works within ENISA as a risk management expert, on various activities in the context of the ENISA's Emerging and Future Risks program, in particular in the area of cloud computing. He is a speaker at information security conferences and editor of the recently published report: Cloud Computing: Benefits, risks and recommendations for information security.

Event Recommendation:

Protection of National Critical Infrastructures in Europe

• Energy • Transport • ICT • Public Security
31st January - 1st February 2011, Berlin, Germany