The European Networks and Information Security Agency - ENISA

KONSTANTINOS VOUDOURIS
Member of ENISA Management Board
Assistant Professor
Department of Electronics
Technological Educational Institute (TEI) of Athens
GR-12210, Athens, Greece
http://www.ee.teiath.gr

Abstract: This paper presents the scope objectives and tasks of the recently established European Networks and Information Security Agency - ENISA. ENISA's mission is to create a platform for a culture of network and information security in Europe, in order to facilitate stakeholders, including EU Institutions and Member States, promote secure solutions in using *e*Networks and *e*Information. Awareness raising as well as promotion of best practices, are among the initial tasks that ENISA will perform, aiming to become a centre of excellence in the area of *e*Security in EU.

Key-Words: Network security, eSecurity, ENISA, .information security, European agency

1. Introduction

Seville European Council summit [1], endorsed *e*Europe 2005 action plan [2]. Vertical actions such as *e*Government, *e*Health, *e*Learning and *e*Business, were based on horizontal once: broadband deployment and eInclusion. The Council, with its Resolution [11], specifically called the Commission to propose concrete measures for the development of culture of security within the member states of the European Union. The Commission introduce to the Council and the European Parliament draft legislation, proposing the formation of a European Networks and Information Security Agency (ENISA). Negotiations between member states and the Parliament started immediately, during the Greek and Italian Presidencies. These negotiations completed in a record time for EU bureaucratic habits, and in March 2004 the relevant legislation came into force [3]. The seat of ENISA was decided during the Brussels European Council (Dec. 2003) to be located in Greece, and followed a decision of the Greek government, ENISA set to be in Heraklion – Crete.

All parties involved, governments, parliament, commission showed a great sense of political will to establish ENISA and have it running as soon as possible. Therefore, Europe could base the development of eServices, on healthy substance and, fulfill the Lisbon agenda, for the most competitive market until 2010.

2. Scope and Objectives

ENISA regulation legal basis, lies within the scope of E.U. market integration [4-11]. Internal market measures require different forms of technical and organisational applications by the Member States and the Commission. These are technically complex tasks with no single, self-evident solutions. The heterogeneous application of these requirements can lead to inefficient solutions and create obstacles to the internal market. This called for the creation of an organisation at European level providing guidance, advice, and when called upon, with assistance within its objectives, inter alia to:

a. ensure high and effective level of network and information security within EU;

b. develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union;

c. contribute to the smooth functioning of the internal market; d. enhance the capability of the Community, the Member States and, as a consequence, the business community to prevent, address and to respond to network and information security problems;

e. provide assistance and deliver advice to the Commission and the Member States on issues related to network and information security falling within its competencies as set out in the Regulation.;

f. building on national and Community efforts, the Agency shall develop a high level of expertise. The Agency shall use this expertise to stimulate broad cooperation between actors from the public and private sectors, and

g. assist the Commission, where called upon, in the technical preparatory work for updating and developing Community legislation in the field of network and information security.

3. Tasks

In order to fulfil its objectives, ENISA shall perform the following tasks:

(a) collect appropriate information to analyse current and emerging risks;

(b) provide the relevant bodies, with assistance within its objectives;

(c)consulte with industry, academia, as well as other sectors concerned and establish networks of contacts for all stakeholder;

(d) facilitate cooperation between the Commission and the Member States in the development of common methodologies to prevent, address and respond to network and information security issues;

(e) contribute to awareness raising by, inter alia, promoting exchanges of current best practices;

(f) assist the Commission and the Member States in their dialogue with industry to address security-related problems in the hardware and software products;

(g) follow the development of standards for products and services on network and information security;

(h) advise the Commission on research related issues as well as on the effective use of risk prevention technologies;

(i) promote risk assessment activities, interoperable risk management solutions and studies on prevention management solutions within public and private sector organisations;

(j) contribute to Community efforts to cooperate with third countries and international organisations;

(k) express independently its own conclusions, orientations and give advice on matters within its scope and objectives.

4. Organisation

The Agency is comprised by:

(a) a Management Board;

(b) an Executive Director,

(c) a Permanent Stakeholders Group,

(d) The staff.The mamagment board is consisted of •31 Members. One per member state, three representing the Commission, and three representing Stakeholders without vote. In the latter group, ICT industry, consumer groups and academic experts are represented equally.

The Executive Director’s responsibilities are:

(a) day-to-day administration of the Agency;

(b) propose draft work programmes;

(c) implement the work programmes and the decisions adopted by the Management Board;

(d) all budget and staff matters;

(e) develop and maintain contact with the European Parliament and for ensuring a regular dialogue with its relevant committees;

(f) develop and maintain contact with the business community and consumers organisations for ensuring a regular dialogue with relevant stakeholders;

The Permanent Stakeholders Group, is consisted of 30 experts. Twenty of them are coming from the ICT industry, 5 from academia and 5 from consumer groups. The main task of this group is to advise the Executive Director in drawing up a proposal for the Agency's work programme, as well as in ensuring communication with the relevant stakeholders on all issues related to the work programme.

When the agency would reach its final formation, 44 members of staff, would have been recruited.

Working groups will be established, in ad-hoc basis whenever the executive director or the management board

The seat of ENISA is in Greece, at Heraklion Crete.

5. Work Program

Trust and security are crucial to the development of society, as information and communication technologies are becoming the backbone of modern economies. Challenges to network and information security are manifold; setting security priorities is becoming an ever more complex and important task for policy makers. The work programme aims to establish a solid and professional infrastructure for practical and advisory work, upon which activities under subsequent work programmes can build.

During the first year of operations, awareness raising and promotion of best practices is the focal point, as well as to establish a network of expertise in member states. ENISA, will activate relevant stakeholders in the Member States and learn from measures already underway. It will develop better understanding of awareness raising and its effects and propagate the measures and their best use. In so doing, the Agency will draft best-practice-material that could be easily customised and presented to Member-States to facilitate their own work on awareness raising.

Furthermore ENISA will:

- promote best practices concerning creation of CERTs/CSIRTs and similar information sharing entities;
- create a number of ad hoc working groups to address topics of common interest;
- set up ad hoc working groups in order to enhance "information sharing" activity related to Networks and Information Security;
- identify best practice for risk analysis and risk management methods, as they vary between sectors and regions and depending on resources;
- collect information on principles and measures taken by the competent National Regulatory Authorities on the protection of integrity and security of data and other forms of malware;
- promote the implementation of a Culture of Security in ICT-related research, in particular such research that is supported by the Commission and Member States;
- engage in fact finding exercises on relevant issues such as integrated wireless networks;
- track information security standardisation activities and help spread information about available standards;
- promote the setting up of CERTs and to discuss trust requirements with existing CERT-cooperation groups;
- facilitate the setting up of networks for rapid dissemination of information on incidents;
- set up contacts with international bodies that are involved in network and information security issues.

6. Conclusions

The establishment of the European Networks and Information Security Agency, (ENISA) is the platform for a culture of network and information security in Europe, in line with *e*Europe 2005 action plan.

First steps would be to provide information and education to establish the required level of knowledge and then to create a positive but realistic attitude to network and information security. ENISA has an important role in this work as it has the means to bring all stakeholders together and identify and develop the channels to disseminate the information and actively promote good practices for managing security risks. It will strive towards achieving a close co-operation amongst the relevant authorities in the Member States, by raising awareness of security problems, establishing common solutions and actively promoting the exchange and use of best practices. This shall facilitate the creation of solutions that take into account experience and expertise from all available sources.

References:

[1] European Council Presidency Conclusions, Seville 21/22 June 2002, No. 13463/02/24-10-2004 (http://ue.eu.int/ueDocs/cms_Data/docs/pressData/en/ec/72641.pdf)

[2] Commission Communication, *e*Europe 2005 action plan", COM(2002)263 and its review COM(2004)108

[3] European Networks and Information Security Agency Regulation No. 460, OJ L 77, 13-3-2004

[4] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services ("the Framework Directive"), OJ L 108, 24.4.2002, p. 33.

[5] Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive), OJ L 108, 24.4.2002, p. 21.

[6] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), OJ L 108, 24.4.2002, p. 51.

[7] Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), OJ L 108, 24.4.2002, p. 7.

[8] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37.

[9] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.1.2000, p. 12.

[10] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178, 17.7.2000, p. 1.

[11] Council Resolution of 18 February 2003 on the implementation of the eEurope 2005 Action Plan OJ C 48, 28.2.2003, p. 2.