enisa
European Network and Information Security Agency

General Report 2007

Executive Summary

European Network and Information Security Agency

ENISA – NIS is people

Networks, people and technology

In the 21st century, we take for granted innovations such as mobile phones, computers, the Internet, on-line banking, e-Health and e-Commerce. The Internet has become indispensable at work and at home. **Network and Information Security (NIS)** is therefore crucial for businesses and home-users alike.

NIS – for Europe's economy

Communication networks and information systems play a central role in the European digital economy and business – both today and increasingly for tomorrow. As networks grow more complex, they also become more vulnerable. Security breaches can generate substantial economic damage. The European Network and Information Security Agency (ENISA) is the European Union (EU)'s response to NIS challenges, especially as they affect the EU's economy.

Expertise and Excellence in NIS

ENISA's role is to be an **expert body and a Centre of Excellence in NIS**. Its mission is to facilitate and support the Members States in enhancing the level of NIS in Europe.

As such, the Agency's role includes:

- Giving **independent, expert advice** to the EU, as the first step towards the drafting of legislation
- **Responding to requests** from Member States and the EU
- **Collecting and analysing** data on security incidents and emerging risks
- Promoting **best practices in e.g. risk assessment and risk management, awareness raising and computer security incident response**

2007 – An Overview

Andrea Pirotti, Executive Director, ENISA

2007 posed considerable challenges for Europe with regard to **Network and Information Security (NIS)**. In particular, the widespread publicity afforded to major cyber-attacks in a number of European countries pushed NIS up on the political agenda. The importance of ENISA's mission, facilitating co-operation and offering support and advice to the EU Member States in their efforts to build protective fences and to implement countermeasures, has become more widely recognised.

By acting as a forum for the exchange of information for all stakeholders, and by increasing co-operation in NIS, the Agency supports the functioning of the Internal Market. ENISA acts to bridge NIS gaps, for example between policy-makers and technical communities, both in the public and the private sectors. The challenges facing Europe are common to NIS policy-makers globally. So ENISA aims to support Europe's policy-makers in giving Europe a leading role internationally in NIS issues.

The ENISA Work Programme for 2007 focused on five priorities:

- Raising awareness and building confidence
- Facilitating the working of the Internal Market for e-Communication
- Mastering emerging technology and services
- Bridging security gaps in Europe in electronic identification (eID), authentication languages, Computer Emergency Response Teams (CERTs)
- Increasing communication and outreach activities.

Activities in pursuit of these five goals were numerous but all of the tasks laid out in the Work Programme for 2007 were achieved on time.

As ENISA nears the end of its first mandate period in 2009, a 'stocktaking' evaluation of its activities featured as an important process in 2007, with strategic discussions regarding future development. In its first three years of operation, the Agency has carved out a crucial position for itself in European NIS and is now well placed to respond to the challenges to come.

The 2007 Work Programme: Key Security Themes

ENISA's work in 2007 concentrated on four themes, which represent crucial NIS objectives for the whole of Europe:

- **Raising awareness and building confidence** – This work is mainly user-oriented, with the aim of improving the safety of network and information security by encouraging the use of appropriate tools and behaviour. In this way, the Agency helps to build the trust that is essential for the acceptance of new technology and the growth of the digital economy.

- **Facilitating the working of the Internal Market for e-Communication** – This objective is oriented mainly towards the needs of business and includes the identification of obstacles to the growth of eCommerce and helping the EU to establish an appropriate mix of regulation and other measures in response to NIS risks.

- **Mastering emerging technology and services** – This technology-oriented task includes not only assessing the impact that emerging technology and services have on security and privacy but also enabling Europe as a competitive supplier of network and information products and services.

- **Bridging security gaps in Europe** – ENISA is helping to analyse gaps in the design and implementation of security tools and procedures throughout Europe, it proposes ways to meet identified needs and monitors developments.

Raising Awareness and Building Confidence

In 2007, ENISA continued to promote awareness raising methods and content, disseminating best practices and promoting security certification schemes. There was a particular focus on countermeasures to combat the threat of spam as an important tool in raising users' confidence.

KPIs for Awareness Raising Campaigns: During 2007 ENISA analysed security awareness practices and metrics to measure awareness, drawing on experiences in the Member States and focusing on case studies of local government and Internet Service Providers (ISPs).

Trends and Progress in Awareness Raising: The Agency gathered new information on current trends and progress in awareness raising, including a detailed inventory of initiatives, focusing on additional target groups: local governments and ISPs.

Dissemination: A dissemination strategy was developed in 2007. To help reach as wide an audience as possible, ENISA released its popular publication, *A Users' Guide: How to Raise Information Security Awareness*, in different languages. More than 2000 copies of awareness publications were given out in 2007, a survey assessing the quality and impact of reports was distributed and the 3rd Awareness Raising Dissemination Workshop was held in Lisbon.

Knowledgebase: In 2007 ENISA extended its 'Knowledgebase' – its centrally stored database of best practices on information security, particularly information security policies – by customising it for more specific audiences.

Information Security Certification: Certification schemes can help to improve the knowledge, skills and confidence of users, especially non-experts. The Agency has made an assessment of the need to facilitate the functioning and accessibility of accreditation and certification schemes and how this could be done in co-operation with the relevant standardisation bodies. A report of its findings has been published.

Security and Anti-Spam Measures of Electronic Communication Service Providers: In 2007 ENISA conducted a new study into the measures service providers take to secure their services and to combat spam.

Facilitating the Working of the Internal Market for e-Communication

Secure electronic communication systems are a major factor governing the development of the Internal Market. ENISA has a key role to play in improving the general level of e-Communication security by identifying obstacles (technical, organisational and cultural) to secure e-Communication and ways to overcome them.

Analysing barriers – a price tag on NIS?

In December 2007, the Agency organised a workshop in Brussels on "Barriers and Incentives for Network and Information Security (NIS) in the Internal Market for e-Communication". The event sought to launch a discussion among relevant stakeholders to collect their input for a report which is aimed at making the economics of security and NIS more visible on the political agenda by putting a 'price tag' on the value of ensuring NIS.

Assessing and Managing Current ICT Risks

ENISA's work on Network and Information Security addresses both current and emerging risks. Current risks refer to the management of contemporary risks that are dealt with using existing Risk Management/Risk Assessment (RM/RA) methods and tools. In this domain ENISA continued the work initiated in 2006 by updating its inventory of RM/RA methods, by looking at additional kinds of current risks in the area of business continuity and by examining the possible integration of RM/RA with other relevant disciplines in the area of technology and governance processes.

The monitoring of NIS standardisation also continued. ENISA has combined forces with the International Telecommunication Union Telecommunication Standardisation Sector (ITU-T) and the Network and Information Security Steering Group (NISSG), to produce an ICT Security Standards Roadmap, a new portal giving Europe a single access point for IT security standards.

Position Papers on Specific Emerging Security Issues

ENISA published three Position Papers in 2007, providing an in-depth analysis of technology-related risks and threats to emerging applications:

Online Social Networks: This position paper starts from the premise that Social Networking is a positive social phenomenon. It provides an introduction to security issues in the area of Social Networking, highlights the most important threats and makes 19 recommendations to reduce the security risks to users.

Reputation-based Systems: Reputation allows users to form an expectation of behaviour based on the judgements of others, bringing the significant economic and social benefits of being able to trust people (or systems) not directly known to the user. This paper provides an introduction to the concept of reputation-based systems, cites cases where they are used successfully, identifies a number of possible threats and attacks and the security requirements they should fulfil, and provides recommendations to help protect users.

Botnets – the Silent Threat: Typically botnets are used for identity theft, unsolicited commercial e-mail, scams, Distributed Denial of Service (DDoS) attacks and other frauds. This paper describes the roles and structures of criminal organisations in creating and controlling botnets, and identifies trends in this type of cyber crime. Online tools to identify and counter malicious code are also included.

Bridging Security Gaps in Europe

In 2007, ENISA's work in this area involved facilitating the exchange of knowledge about incidents and consumer confidence, the exchange of best practices between Member States, the interoperability of electronic authentication systems and helping to bridge gaps in the provision of Computer Emergency Response Teams (CERTs) and similar facilities.

In 2007, ENISA launched its 'European Network and Information Security (NIS) Good Practice Brokerage' for the sharing of experience.

The Agency updated its annually produced Who is *Who Directory on NIS*, extending it with the addition of contacts in the European Institutions, industry and international organisations.

In 2007 ENISA continued to promote the establishment of compatible and interoperable authentication methods through presentations, the publication of papers, a workshop and the creation of an eID directory.

CERTs

ENISA is addressing the problem of how best to approach home-users with NIS information and other means of IT security in a study into the various types of home-users and their perception of the Internet in general and of IT security in particular.

In 2007, the Agency extended the impact of last year's *CERT setting-up guide* with a set of presentation slides which provide an introduction to the whole process of establishing a national response team in the Member States. A good practice collection on how to run a CERT successfully was also produced in 2007, and the Agency organised its 3rd Workshop for CERTs in Europe.

During 2007, the Agency conducted a preparatory study on how certification of CERTs could act as a mechanism for building trust and stimulating communication among the teams. ENISA also undertook a preparatory study into the compilation of standard CERT exercises which will be drawn up in 2008. The aim is for staff in different CERTs to be trained in similar ways, thus paving the way for close co-operation in an emergency situation.

Communication and Outreach

Communications are critically important to the fulfilment of the Agency's objective to foster a 'culture of network and information security'. ENISA co-organised and participated in conferences, seminars and workshops all over Europe, and the international media have reported the Agency's activities and achievements. ENISA upgraded its website, and produced a range of publications including its *ENISA Quarterly* magazine which provides a forum for European debate on NIS. Internal communication, the founding pillar for securing good external communication, was also reinforced. Brand marketing material and brand recognition advertising were commissioned. The first modules in a media training programme for staff were held.

Relationships with Stakeholders

ENISA is a centre of NIS expertise – essential if the Agency is to effectively fulfil its advisory role. ENISA has created a good network of contacts and has established relationships with relevant national industry associations in EU Member States as well as with pan-European industry representative organisations. Various meetings were organised in the Member States, focussing at the beginning of 2007 on visits to Bulgaria and Romania, the new Members of the EU. Since NIS is a global challenge and does not recognise borders, ENISA also participates regularly in the working bodies of international organisations and in 2007 met and discussed global challenges in NIS with representatives from third countries, such as China, Japan and South Africa.

The Agency met with Information Society and Media Commissioner Viviane Reding and with other DGs which have an interest in NIS-related issues – DG Internal Market and Services, DG Enterprise and DG Justice, Freedom and Security. Meetings were also held with representatives of EU Institutions.

To check the effectiveness of its work, the Agency conducted a survey to assess the practical usability of its deliverables in the Member States.

Responding to Requests

In 2007, ENISA received and responded to five new calls for advice and assistance from national governmental bodies.

In addition, the Agency completed its response to a two-part request received in 2006 from the European Commission:

Towards a Data Collection Framework: The objective of this study was to examine the feasibility of creating a partnership of public and private entities, which would benefit from or contribute to a data-sharing initiative for security incidents and consumer confidence, thus providing a pool of knowledge and a firmer basis for decision-making.

The findings of the study and the scope of the problem suggested that one partnership for data collection was not feasible. However, a co-ordinating partnership could tie together existing or new initiatives.

A high-level partnership initiative has therefore been launched. The 'Partnership for ICT Security Incident and Consumer Confidence Information Exchange (PISCE)' aims, through various means, to create an information exchange on IT security and consumer confidence trend data. The partnership was supported initially by ENISA until the end of 2007, with the provision of a public wiki and the hosting of a closed mailing list.

EISAS – NIS Information for Home-users and SMEs: For various reasons, the computers of home-users and SMEs are the most popular victims of targeted attacks. At the same time SMEs are important to Europe's economic growth. However there are gaps in the provision of NIS information to such users. At the request of the European Commission, ENISA therefore embarked on a study into "the feasibility of a European information sharing and alert system (EISAS)".

The findings of the study suggested that the EU should use its position and build on existing resources to foster the establishment of information sharing systems at the national level in Member States.

Change and the Perspectives for 2008

2008 will bring further clarity on ENISA's future role, mandate and potential changes. We look forward to these developments as a means of equipping the Agency for new, European NIS challenges.

The main focus, however, will be on the Work Programme 2008, where ENISA is driving for greater impact through our new Multi-Annual Thematic Programmes (MTPs). These MTPs will run for the next three years (2008-2010) and include.

- **MTP 1 'Improving resilience in European e-Communication networks'** focuses on the identification of current best practices, gap analysis, analysing Internet integrity technologies, and the stability of networks. This MTP will support the review of the EU Electronic Communication Directives.

- **MTP 2 will develop and maintain co-operation models,** in order to use and enhance the existing networks of actors in NIS. In 2008 this MTP will be devoted to
  a) the identification of Europe-wide security competence circles in Awareness Raising and Incident Response
  b) co-operation on the interoperability of pan-European eID and
  c) the European NIS good practice Brokerage.

- **MTP 3 will identify emerging risks for creating trust and confidence.** The Agency will develop a 'proof of concept' of a European capacity for the evaluation of emerging risks, linked to a Multi-Stakeholder Dialogue Forum for public and private sector decision-makers.

Finally, the Agency will undertake a 'Preparatory Action', which includes a feasibility study into the needs of and expectations for NIS in micro-enterprises.

enisa
European Network and Information Security Agency

ENISA – European Network and Information Security Agency
PO Box 1309, 710 01, Heraklion, Greece
Tel: +30 2810 39 12 80, Fax: +30 2801 39 14 10
www.enisa.europa.eu

01/05_08