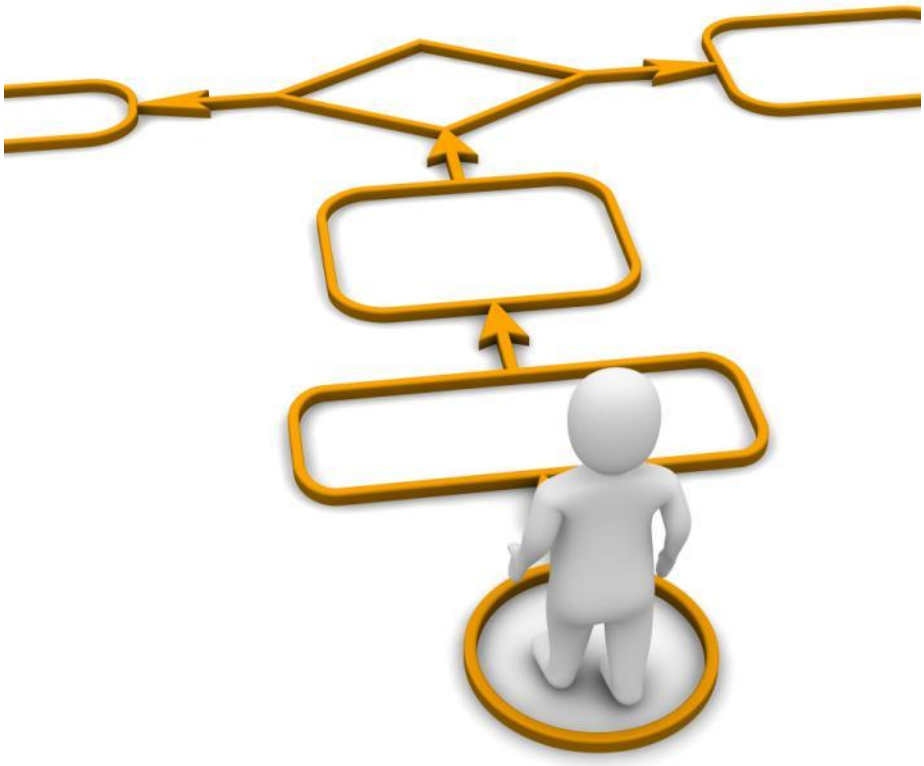
EISAS – European Information Sharing and Alert System for citizens and SMEs

A Roadmap for further development and deployment



enisa
European Network and Information Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

For contacting ENISA or for general enquiries on CERTs, please use the following details:

E-mail: cert-relations@enisa.europa.eu

Internet: http://www.enisa.europa.eu/act/cert/

For questions related to EISAS, please use the following details:

E-mail: eisas@enisa.europa.eu

Background

Citizens and Small and Medium Enterprises (SMEs) constitute the largest group of Internet users in the EU. IT systems owned and operated by these users are popular targets for hackers to, for instance, steal valuable personal information like credit card numbers or customer's details or to be incorporated into botnets, i.e. networks of remotely controlled computers. A botnet, in turn, is the means used to massively distributed spam and malware or to carry out Distributed Denial of Service attacks ("DDoS attacks") against networks.

A successfully conducted DDoS attack will inevitably cause damage for the targeted organisation by causing longer or shorter disruptions of communication services and information systems. In worst case the networks and systems attacked would be part of Critical Information Infrastructures (CII), which makes DDoS attack a serious threat to society at large.

The reason why computers of citizens and SMEs are being targeted by hackers is because the computers of those end-users are generally less protected than those in large organisations and companies. In general, large organisations have more resources at their disposal for managing information security risks including having experts in charge of ensuring the appropriate protection of the organisation's computers and are able to invest in carrying out awareness raising activities and provide training for their employees, i.e. end-users.

Citizens and SMEs on the other hand often lack internal expertise on network and information security and awareness on threats and risks to their computers. Further to this, they often lack the appropriate knowledge about how to protect themselves against those risks and threats.

The EU policy context

In its 2006 Communication on a strategy for a Secure Information Society[1], the European Commission emphasized that public authorities in Member States and at EU-level have a key role to play in keeping citizens properly informed. In this way, they can contribute not only to their own safety and security, but also to a more resilient public communication infrastructure.

In view of its role in fostering a culture of Network and Information Security in Europe, ENISA was requested to "examine the feasibility of a European multilingual Information Sharing and Alert System (EISAS)". EISAS would build upon and link together existing or planned national public and private initiatives. EISAS feasibility study[2] was published in 2007.

The importance of functioning information and alert sharing systems targeting citizens and SMEs was further emphasized, in 2009, by the European Commission in its Communication on Critical Information Infrastructure Protection - COM (2009)149[3]:

> "The Commission supports the development and deployment of EISAS, reaching out to citizens and SMEs and being based on national and private sector information and alert sharing systems. The Commission financially supports two complementary prototyping projects. ENISA is called upon to take stock of the results of these projects and other national initiatives and produce a roadmap to further the development and deployment of EISAS".

Under its pillar on "Trust and Security", the Digital Agenda for Europe[4] stresses the need for Member States to establish, by 2012, a well-functioning network of CERTs at national level covering all of Europe.

EISAS is further addressed in the EU Internal Security Strategy in Action[5]. One of the five objectives aims to raise levels of security for citizens and businesses in cyberspace:

---

[1] *See COM(2006) 251 on a Strategy for a Secure Information Society – "Dialogue, partnership and empowerment": http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:EN:PDF.*

[2] *EISAS feasibility study – final report: http://www.enisa.europa.eu/act/cert/other-work/eisas.*

[3] *See COM(2009) 149 on CIIP - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience": http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:DOC*

[4] *See COM(2010)245 on a Digital Agenda for Europe: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF*

[5] *See COM(2010) 673on the EU Internal Security Strategy in Action at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF*

"Firstly, every Member State, and the EU institutions themselves should have, by 2012, a well-functioning CERT. (…). Secondly, Member States should network together their National/Governmental CERTs by 2012 to enhance Europe's preparedness. This activity will also be instrumental in developing, with the support of the Commission and ENISA, a European Information Sharing and Alert System (EISAS) to the wider public by 2013 (…)".

State of Play

The main findings of the ENISA's study on EISAS feasibility[6] include the following elements:

- There are varying capabilities of Member States (MS) to sustainably reach out to their citizens and SMEs with NIS related information. In the majority (74%) of cases national/governmental CERTs are involved. This predominance of CERTs in that field results from the expertise that these teams have in collecting, processing and sharing of information to conduct their core services of incident response and alerting/warning. Both long-term good IT security practices, and short to mid-term security advices on recent and upcoming threats are provided to citizens and SMEs.
- A centralised solution on European level that directly shares information with the European citizens and SMEs is less likely to be accepted than a solution based on national capabilities. Existing mechanisms and activities must be taken into account and should, even more, contribute to EISAS. The role of ENISA should be that of a facilitator, clearinghouse of good practice information and knowledge- and contact broker.
- MS should entrust their national/governmental CERTs to play a key role in the deployment of EISAS. A successful and accepted deployment of EISAS can only be achieved by well working cooperation between MS in general and their national/governmental CERTs in particular. The possibilities to develop and deploy EISAS within a Public-Private Partnership (PPP) must be explored.

In 2010 ENISA updated its stock taking of existing information sharing and alerting activities in the Member States. In general there is an increasing awareness of the importance to address citizens and SMEs with NIS information and alerts. All known activities operate, as a minimum, a website as distribution channel providing information in the local language.

The two EU-funded prototyping projects FISHA and NEISAS7 will be finalised in the first quarter of 2011. The FISHA project has initiated a network of IT security teams, among them national/governmental CERTs, which have agreed to put into a standard format the relevant security

[6] *EISAS feasibility study – final report:* http://www.enisa.europa.eu/act/cert/other-work/eisas.

[7] *See* http://www.fisha-project.eu/ *and* http://www.neisas.eu/

information that they usually process to inform and alert end-users. They have prototyped a model whereas they share these "information objects" and published them in the native languages of targeted citizens and SMEs.

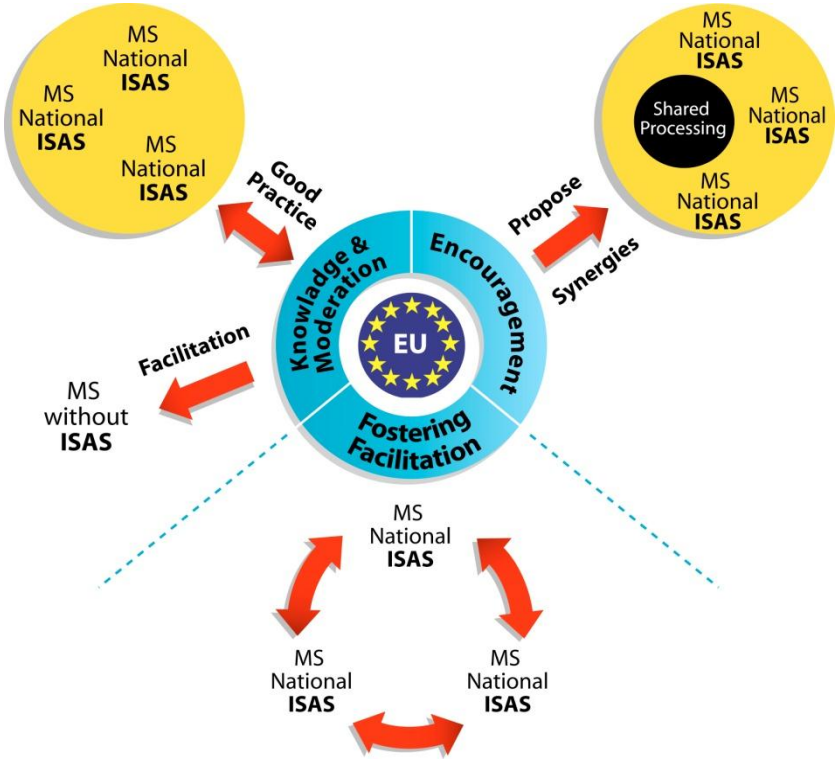
The NEISAS project is complementary as it focuses on increasing cross border synergies between national Network Security Information Exchanges (NSIE). NSIEs are strategic partnerships between public authorities and key private stakeholders, like operators of National Critical Infrastructures, to provide them with additional expertise and information to support their information security process. A pilot between a subset of Member States is under finalisation. NEISAS has also contributed to the emerging ISO/IEC 27010 Information Security Management standard on trusted information sharing.

The Roadmap

Cooperation as the basis

Cooperation between Member States is a precondition for success and the cornerstone upon which this roadmap has been built. EISAS' high-level objective is to empower all EU citizens and SMEs with the knowledge and skills necessary to protect their IT systems and information assets. EISAS will build on national capabilities of EU Member States (including national Information Sharing and Alert Systems – national ISAS).

To that end, the development of well functioning National/Governmental CERTs and a reinforced cooperation between them will be essential. EISAS will be the result and the additional benefit gained from a reinforced cooperation between existing and to-be-built national capabilities. The overall benefit of EISAS is summarised in the figure below.



The role of ENISA

The role of ENISA is to contribute to the implementation of the roadmap by facilitating, supporting and reinforcing the cooperation with and between National/Governmental CERTs as well as other stakeholders from public and private sectors[8].

Next steps

As foreseen by the Digital Agenda for Europe, the establishment, by 2012, of a well-functioning network of National/Governmental CERTs in Europe is essential. Furthermore, National/Governmental CERTs and relevant stakeholders would need to develop, with the support of ENISA, the basic EISAS functionalities required to reach citizens and SMEs.

The relevant services already existing should be brought together to foster discussions on what is needed to further build economy of scale (e.g. in terms of threat analysis, vulnerabilities assessment etc). The findings from the EISAS Feasibility Study, the FISHA and NEISAS projects, and from other existing public and private initiatives need to be considered. Architectural aspects have to be analysed by leveraging on existing functions, protocols, procedures, templates and mechanisms and by identifying what needs to be further developed, in particular, to ensure interoperability between national ISAS services.

As an intermediary step, it can be envisaged to build upon regional/smaller group level cooperation to stimulate the overall EU engagement. A trial can be envisaged for 2012 to enlarge the existing prototyping to a broader community of Member States. It is to be noted that financial support is made available, on a needed basis, via the financing scheme of the European Programme for Critical Infrastructure Protection (EPCIP)[9] whereas priority is given to advancing the development and deployment of EISAS.

The objective is to deploy EISAS by 2013. In the long term, synergies need to be envisaged between EISAS and the CERT for the EU Institutions to be established by 2012. In summary, the EISAS roadmap builds on the activities indicated in the table below.

---

[8] *For more details on the activities in 2011, see the 2011 ENISA Work Programme:* http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/enisa-work-programmes-general-reports

[9] *See the Annual Work Programme for 2011 for the specific programme on "*Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks*":* http://ec.europa.eu/home-affairs/funding/docs/C20108325EN.pdf

Activities	Timeline
Establishment of a well functioning national/governmental CERT **in each MS**	**End of 2011**
Reinforce cooperation **between national/governmental CERT towards a well-functioning network of National/Governmental CERTs in Europe by 2012**	**2011-2012**
Development of EISAS basic functionalities and services	**H1 2011**
Integration of ISAS capabilities **in National/Governmental CERT services**	**2011-2012**
Development of customized services **in order to meet particular MS' needs**	**H2 2011**
Development of interoperability services **for national ISAS in order to enable the deployment of EISAS**	**H2 2012**
Trial among a subset of EU MS **to stimulate the overall EU engagement**	**H2 2012**
Deployment of EISAS **in the EU**	**2013**