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

Implementation through cooperation

enisa
European Network and Information Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) acts as a centre of expertise on cyber security for the European Union (EU), its Member States (MS), the private sector and Europe's citizens. As an EU agency, ENISA's role is to work with all of these stakeholder groups, as well as the academic world, to develop advice and recommendations on good practice in computer security. The agency assists MS in implementing relevant EU legislation, and works to protect Europe's critical information technology networks through activities such as pan-European cyber security exercises. In addition, ENISA acts as a 'switchboard' for exchanging knowledge among all of its stakeholders.

Contact details

The editor of this report was Mr Kjell Kalmelid, Expert, ENISA. For questions related to this report, EISAS or for general enquiries on CERT Cooperation, please use the following contact details:

E-mail: CERT-Relations@enisa.europa.eu

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

List of contributors

This paper was produced by the ENISA editor using input and comments from a group selected for their expertise and experience in the subject area.

The views expressed in this publication are those of the editor, unless stated otherwise, and do not necessarily reflect the opinions of the participating Experts.

Pascal Steichen	Ministry of Economy (LU)
Otmar Lendl	CERT-AT
Kauto Huopio	CERT-FI
Raoul Chiesa	CLUSIT (IT)
Ioannis Askoxylakis	FORTHcert (GR)
Tony Neate	GetSafeOnline (UK)
Tore Larsen Orderløkken	NORSIS (NO)
Andrew Cormack	JANET (UK)
John Harrison	LanditD and NEISAS
Ulrich Seldeslachts	LSEC (BE)
Peter Burnett	Quarter House Ltd.

Executive summary

This report contains considerations and suggestions on how to further support the Member States in deploying the European Information Sharing and Alert System (EISAS). This report implements the foreseen activities in the ENISA Work Programme of 2011[1] and paves the way for the implementation

[1] http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/work-programme-2011

of the 2012 activities that were pointed out in the EISAS Roadmap.[2] The goal of this report is to provide input to future activities aiming at further developing the recommendations of the FISHA[3] project including, but not limited to, those of ENISA.

Several Experts were interviewed to give their opinion on EISAS. They are representing European National/Governmental CERTs ('Nat/Gov. CERTs'), organisations active in raising information security awareness among citizens and SMEs ('non-CERTs') in their countries or are independent with long experience in the area of trusted information sharing and exchange.

The result of the interviews revealed that the idea of EISAS is supported by Experts representing both Nat/Gov. CERTs and non-CERTs. However, in the discussions on EISAS from different perspectives, those from non-CERTs were generally more enthusiastic about EISAS than those from Nat/Gov. CERTs. This is mainly due to the fact that Nat/Gov. CERTs will need funding if a meaningful engagement in EISAS is to be realised.

The non-CERTs consider EISAS as a way of exchanging ideas and experiences on a European level since a community for these organisations and initiatives does not really exist. They are very positive to contribute to the development of EISAS by participating in a possible large-scale pilot of the EISAS Basic Toolset in 2012. So are the Nat/Gov. CERTs, but they are much more cautious and reiterate the importance of obtaining funding as a condition for their participation.

All the Experts agree that targeting citizens is different from targeting SMEs. For citizens a concept such as the EISAS Basic Toolset is definitely worthwhile to further develop. For SMEs, and particularly medium-sized enterprises, it appears to be a better approach to apply the concept of WARPs (Warning, Advice and Reporting Points), which are information-sharing communities based on a model developed by the UK government CPNI [4](formerly NISCC).

On the issue of management of EISAS, the model proposed by FISHA was generally seen as feasible, but there were no strong opinions on this matter. Most of the Experts believe priority must be given to the development of activities for cross-border cooperation on issues concerning information sharing

---

[2] *In addition, it provides a detailed background of EISAS. 'EISAS - Roadmap for further development and deployment', ENISA, 2010: http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap*

[3] *All information about the FISHA project is available at the project's website: http://www.fisha-project.eu*

[4] *For more details check http://www.cpni.gov.uk/*

and exchange. Finally, the Experts see at least partial funding from the governments as a precondition for realising EISAS.

Introduction

The EISAS Roadmap anticipates that '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'. Furthermore it states that:

'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[5] projects, and from other existing public and private initiatives need to be considered'.

This report builds on the aforementioned findings and, additionally, on discussions held with members of an Expert Group[6]. The group comprised 11 persons representing National/Governmental CERTs in Europe and organisations active in raising information security awareness among citizens and SMEs in their countries. Each individual was invited for a phone interview by the author of this report.

The interviews were conducted from 5 to 15 September 2011. As a basis for the discussion, and to ensure consistency, a questionnaire[7] with 14 questions was used. Since the intention was to allow for a broader discussion on the various issues, all questions were open. Each interview lasted for about 45-60 minutes, but all individuals were given the option to convey their opinions in writing if they so wished.

The objective of the discussions was primarily to obtain a deeper understanding of what is required to enable the implementation of EISAS. In other words, the objective was to identify concrete opportunities and obstacles for such implementation. The objective was also to explore the possibilities of gaining support for the EISAS Basic Toolset approach in its first version.

---

[5] *All information about the NEISAS project is available at the project's website: http://www.neisas.eu/*

[6] *Please see Page 3: List of contributors.*

[7] *Please see Annex 4-2 for details about the questionnaire.*

Results

1.1 The FISHA management model

The FISHA consortium has proposed a management model with four players ('the FISHA Model'):

- Network Security Organisations;
- Information Producers;
- Local Information Brokers;
- Information Consumers (i.e. Citizens and SMEs).

The 'Network Security Organisations' are central in this model as they would be the main stakeholders for running a national Information Sharing and Alert System ('National ISAS'). The producers and brokers are certainly critical, but complementary to the network security organisations. According to this model, Nat/Gov. CERTs as well as other organisations with a mission to target citizens and/or SMEs in the Member States would fall within the category of network security organisations even though, to some extent, they are also producers and brokers of security information.

Furthermore, the FISHA project proposed two kinds of node to be established for administering the cooperation between these players: a Central node and several Basic nodes. From a technical-administrative point of view, the network security organisation representing the Central node would, among other things, be responsible for managing the network of Basic nodes. To that end, the FISHA project had developed a web application prototype ('the FISHA System'), which also builds on P2P technology for sharing information in the network. The Central node would also be the interface to other Central nodes in other countries.

The combined activities carried out by the Central node and the Basic nodes can be described as the national ISAS. Regardless of whether or not the Central node is a CERT, the role entails taking responsibility for the running and coordination of the national ISAS.

1.2 Considerations on the idea of EISAS

The high-level objective of EISAS is to empower all EU citizens and SMEs with the knowledge and skills necessary to protect their IT systems and information assets. EISAS is supposed to build upon and link together existing or planned national public and private initiatives. Nat/Gov. CERTs should also play a role in the realisation of EISAS.

With this description of EISAS, the Experts were initially asked for their general opinion on the idea. When it comes to the overall objective of EISAS, everyone agreed this is a highly important task for every Member State to perform. However, when the discussion went into the issue of *how* EISAS

should be implemented as a means of sharing targeted security information to citizens and SMEs, it is clear that the following factors need to be addressed:

- the roles and operational conditions of Nat/Gov. CERTs vis-à-vis other organisations within the frame of the FISHA model;
- the FISHA prototype web application ('the FISHA System');
- the differences between the EISAS target groups, i.e. citizens and SMEs respectively.

1.3 Roles and operational conditions

1.3.1 Nat/Gov. CERTs

The Expert Group were asked which of the two roles – Central or Local node – they see as most fit for the Nat/Gov. CERT to play within a national ISAS in their country. They were, additionally, asked to respond in view of the division of roles and responsibilities for awareness-raising in their country.

Experts from Luxembourg, the UK and Norway answered that they did not regard the Nat/Gov. CERTs as a suitable player for this role in their country whatsoever. The reasons they gave as the basis for this view were *scope* and *focus*. CERT representatives generally shared the view that, to some extent, scope and focus pose a challenge when it comes to engaging in EISAS. However, the main issue in terms of taking the responsibility for an ISAS as a Central node is that of *resources*. The operational conditions *scope, focus* and *resources* are briefly presented below.

- **Scope**
  Although many Nat/Gov. CERTs do target citizens and SMEs, far from all CERTs target those groups alone. Some countries have several publicly funded CERTs, none of which have citizens and SMEs as their target group. In such countries, other initiatives have been established to address the needs of citizens and SMEs to obtain security information.
- **Focus**
  The primary task of the CERT is to *respond to* and *coordinate the handling of* incidents. Their main focus is not to *proactively* stop incidents from happening, but to *react* when an incident has occurred; the so-called 'Digital Fire Brigade' task.
- **Resources**
  It is a fact that Nat/Gov. CERTs are generally very small organisations with fewer than ten and in some cases fewer than five employees. This circumstance makes it difficult for most of them to engage in anything other than the core business.

If the FISHA System is to be integrated into EISAS, the representatives of CERT.at, FORTH CERT and CERT-FI all consider their organisation as the most realistic option for running the Central node in their countries respectively. They are open to further developing their *proactive* activities, but unless funding can be secured they simply have no or very limited possibilities to develop or engage in any such activity, EISAS included.

1.3.2 Other organisations

The Expert Group were also asked: a) which other organisations/initiatives should be considered part of a national ISAS in their country, b) if these organisations could be defined as network security organisations and c) to what extent they would be suitable to represent the Central node in the country.[8]

It was clear that in the countries where the Nat/Gov. CERT is not seen as the most relevant organisation, there was at least one alternative organisation established in that country. If the FISHA System is to be integrated into EISAS, the Experts representing non-CERT organisations all consider themselves as suitable candidates for being the Central node in their country. The organisations that participated in this survey are briefly presented below:

- The main mission for L-SEC[9] – a not-for-profit association in Belgium – has been to create IT security awareness for industry at large, and their members are primarily SMEs. Nonetheless, L-SEC could definitely consider being the Central node in Belgium as the security information it distributes to SMEs often covers the needs of citizens as well.
- CLUSIT[10] in Italy is also a not-for-profit association and is open to both individuals and organisations. Their mission is to raise the computer security culture among companies, public administrations and citizens. CLUSIT is a well-renowned and respected organisation in Italy. It has excellent relations with both industry and the Italian government.
- CASES[11] in Luxembourg, NorSIS[12] in Norway and GetSafeOnline[13] in the UK are all partly funded by their governments and have very similar tasks and target groups. NorSIS and GetSafeOnline rely on additional funding from the private sector.

---

[8] In those cases where the Experts actually represented such an organisation, the question was rephrased to apply to their own organisation.

[9] For more details about L-SEC please see the organisation's website: http://www.lsec.be/

[10] For more details about CLUSIT please see the organisation's website: http://www.clusit.it/

[11] For more details about CASES please see the organisation's website: http://www.cases.public.lu/fr/index.html

[12] For more details about NorSIS please see the organisation's website: http://www.norsis.no/

[13] For more details about GetSafeOnline please see the organisation's website: http://www.getsafeonline.org/

1.4 CERTs and the FISHA System

The main deliverable of the FISHA project was a web application prototype for information sharing and alerts ('the FISHA System'). But at the closing workshop[14], the use of the FISHA System raised a number of questions and, to some extent, also concerns[15]. Mainly, it was unclear what information was supposed to be processed and shared in the system.

A comment from one Expert in this survey was that if the FISHA System is used for *processing* information as it arrives (input), the potential benefits for EISAS would be that it saves time. However, since the processed information is intended to be distributed to citizens and SMEs or published (output), it is by definition *open*.

Hence, the potential usefulness of the system ends as soon as the information is processed. As another Expert commented, the system is to a large degree 'over-engineered'. If open information is the output, then there is no real need for a secure resilient distribution infrastructure based on P2P technology. On the other hand, if the information would be restricted then the FISHA System to some extent competes with other, already existing channels for sharing information. It was also remarked that the idea of translating security information to English prior to sharing it is challenging. Regardless of whether there are many small or a few large pieces of text, it will inevitably require time and resources to translate them.

In contrast to this quite sceptical view of the FISHA System, more than one Expert emphasised that the FISHA System could be potentially very useful if used for 'co-analysing' information. Basically, every CERT uses the same information sources and subscribes to the same mailing lists and RSS-feeds in order to monitor security events on the web at large. Those activities could be shared by several CERTs, thus synergies can be achieved.

A 'co-analysing' project like this, however, requires both mutual trust among CERTs and respect for the technical expertise of the provider of an analysis. If successful, it might be a way for Nat/Gov. CERTs to actually release resources for other activities, for example, more 'proactive' ones. Moreover, to share the burden of processing information would facilitate another objective of EISAS, namely to reinforce

---

[14] *See 'Minutes of the FISHA project closing workshop':*

http://fisha-project.eu/sites/default/files/FISHA_closing_workshop_minutes.pdf

[15] *See also EISAS Basic Toolset report, (ENISA, 2011) for further details on ENISA's view on EISAS implementation.*

cooperation between CERTs. One Expert said that although attempts to share the burden of processing of information among CERTs have been made in the past with little success, it should not stop the CERT community from trying again.

1.5 Targeting citizens & SMEs

In the discussions on the EISAS Basic Toolset, it became clear that targeting citizens is quite different from targeting SMEs. In addition, it was remarked that there are also differences between micro, small and medium enterprises that must be taken into account.

1.5.1 EISAS Basic Toolset

Two questions were about the EISAS Basic Toolset. This is an ENISA activity which is part of the ENISA 2011 Work Programme. It falls within the overall role of ENISA to facilitate the development of EISAS, it is an activity foreseen in the EISAS Roadmap as 'Development of EISAS basic functionalities and services' and aims at contributing to the 'outreach challenge' in the FISHA proposal for communication channels. That proposal recognised the need for 'something' in between information producers and the information consumers, but during discussions at the FISHA closing workshop it was unclear what this concretely could be apart from local information brokers.

The idea that ENISA has piloted – and named EISAS Basic Toolset – was to reach out to home users, i.e. citizens, at their workplace instead of addressing them at their home. At the interviews, the Experts were informed that preliminary results of the pilot were very promising in terms of *impact,* i.e. changes in knowledge, attitude and behaviour of the home users.

All the Experts said that if the preliminary results can be verified when the pilot has ended, it would definitely be worthwhile to develop the EISAS Basic Toolset concept further. All five Experts representing the non-CERT organisations, CASES (LU), GetSafeOnline (UK), CLUSIT (IT), L-SEC (BE) and NorSIS (NO), also expressed a strong interest in taking part in a large-scale pilot of this approach in 2012. CERTs were more 'carefully positive' to the idea of taking part in a large-scale pilot, provided costs are covered.

1.5.2 Value of performance indicators

An essential requirement for the development of the EISAS Basic Toolset was that the results of the pilot would be validated. The preliminary results presented to the Experts were all validated through a set of performance indicators on knowledge, attitude and behaviour of the home users and thus demonstrated that the approach can lead to concrete effects.

The Experts were asked for their opinion on the value of obtaining such indicators as a result of targeting citizens with information on how to improve security. The Experts responded that they believe such indicators would be very useful. They point out that producing results is, of course, a condition in order for any organisation or initiative to obtain funding. If you can demonstrate success then raising funds is much easier. One Expert said that measuring concrete effect on set performance indicators should be integrated as a component in EISAS.

1.5.3 Targeting micro and small enterprises

In the discussions, the Experts made remarks on the differences between the EISAS target groups, i.e. citizens and SMEs, and how important it was to take those differences into account when targeted. With regards to citizens, there are numerous factors that make it practically pointless to target them as one and label them 'home users'. Differences in age and educational levels are just a few examples of the characteristics of home users. The EISAS Basic Toolset pilot recognised these differences by restricting its scope to those home users that are also *non-manual workers*, in other words, focusing on reaching out to adults of approximate age 24-65 with medium or high education.

With regard to SMEs, micro, small and medium are basic characteristics of size[16]. However, from the perspective of successfully sharing security information with SMEs, the size does not seem to be what matters most. What seems to be a more important factor is their ability to grasp and comprehend security information. Many Experts say this ability is more linked with the ICT dependency than with the size of the company. Consequently, there are small companies with better ability to consume security information than medium-sized ones.

In general, however, this ability is linked to the growth of the company in terms of size. At a certain point in time of its evolution, a company needs to address development, maintenance and support of its ICT more strategically. Regardless of whether that need is addressed by hiring someone with the required skills or by outsourcing its ICT operations, the level of the company's ICT maturity increases.

One Expert says micro-enterprises are considered one of the hardest communities to reach and provide actionable information to. Yet another one says the way to addressing micro-enterprises is to make it even easier for them to take security measures and added that these enterprises are not

---

[16] *According to the EU definition on sizes of SMEs, micro enterprises are defined as fewer than 10 employees, small enterprises as fewer than 50 and medium-sized enterprises as fewer than 250.*

http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm

interested in what the threats or vulnerabilities are and how they can damage their computers, they simply want to know which button to push in order to make things work smoothly.

1.5.4 The WARP concept

In the discussions on how to better reach out to SMEs within EISAS, many Experts referred to the British WARP (Warning, Advice and Reporting Point) initiative. The WARP programme is part of the Information Sharing Strategy of the Centre for the Protection of National Infrastructure (CPNI)[17]. According to CPNI, 'a *WARP is complementary to CERTs, helping to deliver advisories more effectively to small subsets of the CERT's constituency and promote information security among organisations the CERT cannot reach on its own'.* This suggests that WARPs fit pretty well in the FISHA model as information brokers. The FISHA model anticipates information brokers to be connected to network security organisations such as CERTs through the FISHA System.

With regards to those SMEs that have a higher level of ICT maturity and thereby a better understanding of the importance of information security, the WARP model could very well be the channel CERTs are looking for to better reach out to those target groups. It may not be an easy task to define 'ICT maturity' from a security perspective, nor which SMEs would be suitable to target. Nevertheless, it should be worth discussing if and how the WARP model could somehow be integrated into EISAS.

1.6 Management and funding of EISAS

The FISHA project proposed the following governance model:

- There would be a Steering Committee, which adopts a policy of the 'FISHA Network', i.e. EISAS.
- The Steering Committee would decide:
  - who can become a member of the network;
  - what will be its role;
  - who will additionally work in the Core Network (offer the necessary services and responsibility).

[17] *The website of WARP is located at: http://www.warp.gov.uk/*

At the FISHA closing workshop, it was not possible to agree on which organisations should form the Steering Committee and on what basis.

The Experts were asked for their views on FISHA's proposal for a management model and also on the issue of funding. With a few exceptions, no strong feelings were expressed on that model. All Experts had long experiences of international cooperation on information sharing and exchange. They envision a future Steering Committee as a relatively small group of individuals dealing only with pure strategic issues. All operational matters should be left for the participating organisations in the Member States respectively to decide on.

Having all Member States represented was generally not seen as feasible. On the other hand, as one Expert said, it is probably necessary that the Central node organisations are represented in the committee. Another Expert said the sensitivity of the information to be exchanged inevitably will affect the management model of EISAS. If trust is to be a significant factor for any sharing to take place, the TF-CSIRT approach may be considered as a model for coordinating and managing the cooperation. It should be noted that the vast majority of the Experts agreed that before any cooperation has started, the issue of management is critical.

Most Experts said that in order for EISAS to be realised, the governments have to support the initial funding of EISAS. One Expert said the success and organisation of the Safer Internet programme with nodes in every Member State would have taken much longer to achieve without strong support and funding from the governments. The role of ENISA should remain that of a facilitator and driver.

Conclusions

From the discussions with the Expert Group the following can be concluded:

- There is a general support of the idea of **EISAS as a cooperation model** for targeting citizens and SMEs with security information.
- The operational conditions of Nat/Gov. CERTs in terms of *scope, focus* and *resources* seriously challenge the idea of building on **Nat/Gov. CERTs as the Central node** and driving force for EISAS in the Member States. For Luxembourg and the UK, this is obviously not an option. In other Member States this may be an option or even the only option and it demonstrates the complexity of the issue.
- The Nat/Gov. CERTs interviewed say the FISHA System may be used for **co-processing/co-analysing information** and that opportunity should definitely be further investigated, not least because of the high potential of the activity to reinforce cooperation among Nat/Gov. CERTs.
- With regards to targeting home users and on the basis of preliminary results of piloting the **EISAS Basic Toolset**, non-CERTs from five countries, Belgium, Luxembourg, Italy, Norway and

the UK, expressed a strong interest in participating in a large-scale pilot of this concept in 2012. Two Nat/Gov. CERTs would also be willing to participate provided funding is secured.

- Experts agreed that **micro and small enterprises** generally do not have the skills, time or resources to absorb very detailed security information and only want to know 'which button to push'. The main problem concerning these target groups is not the quality of the security information, but **how to reach them** and convince them of the value of taking part in that information exchange.
- Most **medium enterprises** have some sort of internal ICT coordination and are therefore more likely than not to gain from and have the ability to absorb more detailed information. The **WARP model seems to be a good way** of transmitting such information to medium enterprises.
- Ideally, EISAS should develop into a **network between organisations/initiatives** targeting citizens and SMEs similar to that of Safer Internet. In other words, EISAS should get minimum funding from the Member States for setting up nodes throughout Europe.

Annexes

4-1 Annex A: Acronyms

EISAS – European Information Sharing and Alert System

ISAS – Information Sharing and Alert System

NEISAS – National & European Information Sharing & Alerting System

FISHA – Framework for Information Sharing and Alerting

P2P technology – Peer-to-Peer technology

WARP – Warning, Advice and Reporting Point

CERT – Computer Emergency Response Team

4-2 Annex B: Questionnaire

The questionnaire was composed of 14 questions divided into three main topics:

- EISAS and national ISAS;
- the role and responsibilities of the Nat/Gov. CERT;
- discuss EISAS Basic Toolset and support of that concept including gathering of statistical data on the security of home users.

Questions

1. What's your opinion on the idea of EISAS?

2. From the perspective of the division of roles and responsibilities for awareness-raising in your country, which of these roles do you see as most feasible for the CERT to play within a national ISAS in your country?

3. What's your opinion on this idea of having the CERTs taking the lead in realising EISAS? Is it realistic? If not, why? What is required to realise it?

4. Given that EISAS targets citizens and SMEs, which other actors should be included in the operations of a national ISAS?

5. Could you please provide us with some names of two such actors?

6. On this background, what is your general impression about this approach and possibility to integrate in the EISAS concept?

7. Would your organisation be willing to take part in a large-scale pilot of this approach in 2012?

8. What about other actors in your MS. What are the chances they would be willing to participate in such a pilot?

9. What is your opinion on the value of the stats produced? Could such data be useful for your organisation (regardless if it's part of EISAS or not)?

10. Do you have any opinions/suggestions on which organisations should form the Steering Committee?

11. Is it important that the organisation running the Central node in an MS is a member of the SC?

12. Do you have any suggestions to make/comments on the possible criteria/requirements to be fulfilled in order to be part of the SC?

13. What role, if any, should ENISA play for EISAS?

14. Do you have any opinions/suggestions on the long-term funding of a future EISAS? Who should be the main sponsor?

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu