ENISA and CERTs

Results from 2006
A wrap-up and outlook

Marco Thorbruegge, ENISA
Senior Expert Computer Security and Incident Response

2nd ENISA Workshop CERTs in Europe
05th October 2006
Table of Content

• Overview of ENISA
• ENISA and CERTs
Overview: ENISA Facts

- ENISA: European Network and Information Security Agency
- Operational since September 2005
- Headquarters: Heraklion, Crete, Greece
- Staff: 1 Executive Director, 3 Heads of Department, 20 Experts and 1 Seconded National Expert
Overview: ENISA’s Objectives

- To **enhance** the **capability** of the Commission, other EU bodies and the Member States to prevent, address and to respond to NIS problems.

- To **provide** **assistance** and deliver **advice** to the Commission and the MS on issues related to NIS falling within its **competencies** as set out in this Regulation.

- To **develop** a high level of **expertise** and use this expertise to **stimulate** broad **cooperation** between actors from the public and private sectors.

- To **assist** the Commission, where called upon, in the technical preparatory work for updating and developing Community legislation in the field of NIS.
Overview: ENISA structure

Organisational Chart of the European Network and Information Security Agency
Table of Content

• Overview of ENISA
• ENISA and CERTs
ENISA & CERTs: Mission

(Source: Job description)

- Promote and facilitate good practice in setting-up and running of CSIRTs / WARPs / Abuse Teams / etc.
- Encourage cooperation between different actors, especially between policy makers and “implementers”
- Develop relations to the various CERT communities
- Support their activities
- Run an ad-hoc Working-Group with external experts
ENISA and CERTs

The Big Picture

2005 Stocktaking
2006 Setting up & Cooperation
2007 Support operation (+ broaden focus!)
- Quality assurance
- Advanced Training
Prepare to contribute to “NIS marketplace”!
2008 Finalise basic work
A sound set of basic documents should be available now.
The FUTURE:
Now extensively collect good practices and contribute to NIS marketplace!
ENISA and CERTs

ENISA’s Inventory of CERT activities in Europe

2005: Stock-Taking
ENISA and CERTs

2005: Stock-Taking

Also online: http://www.enisa.europa.eu/cert_inventory/
ENISA and CERTs

1st Workshop CERTs in Europe

2005: Stock-Taking
ENISA and CERTs

2006: Setting-up & Cooperation

- Facilitate training
- Examine tools
- Promote ideas

[...]
ENISA and CERTs

Step by step approach...: Structure

• Overall strategy for planning and setting up a CSIRT
• Developing the Business Plan
• Promoting the Business Plan
• Examples of operational and technical procedures (workflows)
• CSIRT training
• Exercise: producing an advisory
• Description of the Project Plan
ENISA and CERTs

Complete but concise process description

- Only around 80 pages
- Illustrated (next slide)
- Generic enough to serve several target groups
- A lot of references to other sources
- Based on “real life” experiences

2006: Setting-up (2)
ENISA and CERTs

Illustrations
Workflows, Models, Statistics,…

2006: Setting-up (3)
ENISA and CERTs

Wrap-ups, examples and exercises

We have taken the following steps so far:

1. Understanding what a CSIRT is and what benefits it might provide.
2. To what sector will the new team deliver its services to?
3. What kinds of services a CSIRT can provide to its constituency.
4. Analysis of the environment and constituents.
5. Defining the mission statement.
6. Developing the Business Plan.
   a. Defining the financial model.
   b. Defining the organisational structure.
   c. Starting to hire staff.
   d. Utilising and equipping the office.
   e. Developing an Information security policy.
   f. Looking for cooperation partners.
7. Promoting the Business Plan.
   a. Have the business case approved.
   b. Fit everything into a project plan.
8. Making the CSIRT operational.
   a. Creating workflows.
   b. Implementing CSIRT tooling.
9. Training your staff.

>> The next step is to exercise and be ready for the real step.

Fictitious CSIRT (step 3a)
Making an analysis of the constituency and the appropriate communication channels

A brainstorming session with some key persons from management and the constituency generated enough input for a SWOT analysis. This lead to the conclusion that there is a need for the core-services:

- Alerts and warnings
- Incident handling (analysis, response support and response coordination)
- Announcements

It must be ensured that the information is distributed in a well-organised manner to reach a biggest possible part of the constituency. So the decision is made that alerts, warnings and announcements in the form of security advisories will be published on a dedicated website and distributed via a mailing list. The CSIRT facilitates e-mail, phone and fax for

<table>
<thead>
<tr>
<th>Bulletin Identifier</th>
<th>Microsoft Security Bulletin MS06-042</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulletin Title</td>
<td>Cumulative Security Update for Internet Explorer (918899)</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>This update resolves several vulnerabilities in Internet Explorer that could allow remote code execution.</td>
</tr>
<tr>
<td>Maximum Severity Rating</td>
<td>Critical</td>
</tr>
<tr>
<td>Impact of Vulnerability</td>
<td>Remote Code Execution</td>
</tr>
<tr>
<td>Affected Software</td>
<td>Windows, Internet Explorer. For more information, see the Affected Software and Download Locations section.</td>
</tr>
</tbody>
</table>
ENISA and CERTs

Project plan (separate file)

2006: Setting-up (5)
ENISA and CERTs

Facilitate cooperation: Structure

- Analysis of the relevant stakeholders
- What does cooperation mean?
- What are the incentives, benefits and barriers?
- Past and present of (CERT) cooperation
- The future: what can the stakeholders do to enhance cooperation

2006: Cooperation
ENISA and CERTs

2007: Support existing teams

- Continuity: continue 2006 work
- Add value: good practice for successfully serve your constituency
  - Quality assurance
  - Advanced training
  - Exercises
  - ...
- Change focus (next slide)
ENISA and CERTs

2007: Change focus (a bit)

CERT

Focus on CERT/CSIRT

Academic

SME

[...]

Government

End User

Research

CERT

ABUSE TEAM

Focus on the User (-groups)

Government

(Type of)

Users

WARP

Vendors

[...]
ENISA and CERTs

Ad-hoc Working Group already works on preparation for 2007:

• Analysis of (user-)groups
  • Analysis of user-needs for specific (CSIRT-)services
  • What is the appropriate provider for these services
  • Goal: enable more granular analysis; help MS to identify gaps
• List with possible measures for quality assurance

Additional work:

• List with publicly available security information

2007: Preparation in 2006
ENISA & CERTs: The Big Picture (I)
BASIC WORK (Horizon end of 2008)

2005 Stocktaking

2006 Setting up & Cooperation

2007 Support operation (+ broaden focus!)
- Quality assurance
- Advanced Training

Prepare to contribute to “NIS marketplace”!

2008 Finalise basic work

A sound set of basic documents should be available now.

The FUTURE:
Now extensively collect good practices and contribute to NIS marketplace!
ENISA & CERTs: The Big Picture (II)
INVolvement in the security communities (Horizon ongoing)

We are in close contact with all these since 2005!
ENISA & CERTs: The Big Picture (III)
THE PREQUESITION FOR SUCCESS IN SHARING INFORMATION (esp. GOOD PRACTICE):

TRUST!

ENISA must establish a trusted relation to potential suppliers of information (esp. good practice) through:

• Involvement (Be present! Contribute! Support!)
• Competence (Develop expertise! Deepen expertise! Advertise it!)
• Transparency (Publish! Present! Talk! Share!)

Why?
Especially CERT-people are security-allrounders!

For the “NIS marketplace” contribution from the several security communities (not only CERT!) is crucial!

-> Foster the relationships! Keep the overview! Be trustworthy!
Stay in touch with ENISA!

Go to our website: 
http://www.enisa.europa.eu

Subscribe to our Quarterly Newsletter:

To subscribe to the ENISA Quarterly, please mail to press@enisa.eu.int, and clearly state "NEWS" (!) as subject.
Stay in touch with ENISA!

Meet us in Rome!

Visit us in Heraklion!
European Network and Information Security Agency
Science and Technology Park of Crete (ITE)
Vassilika Vouton,
70013 Heraklion, Greece
Thank You!

Contact:
Marco THORBRUEGGE
Senior Expert Computer Security and Incident Response
Cooperation and Support Department
+30.2810.39.1372
marco.thorbruegge@enisa.europa.eu