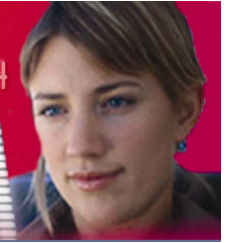


ENISA update

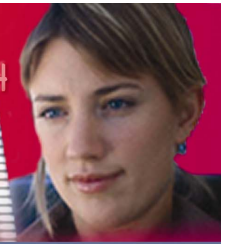
Marco Thorbruegge, ENISA
Senior Expert Computer Security and Incident Response

19th TF-CSIRT
21-22 September 2006 Finland



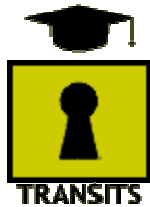
ENISA – in a nutshell

- Center of Expertise for the MS governments and EU bodies
- Established in 2004, moved to Crete/Greece in 08/2005
- First Mandate ends 10/2008
- Mid-term review started; results in 04/2007
- Topics:
 - CERT
 - Awareness Raising
 - Risk Management
 - Security Policies
 - Security Technologies
 - Relations to Stakeholders



ENISA and CERTs

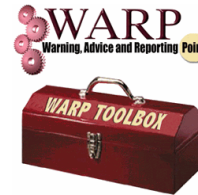
2006: Support new teams



Facilitate training



Examine tools



Promote ideas

[...]

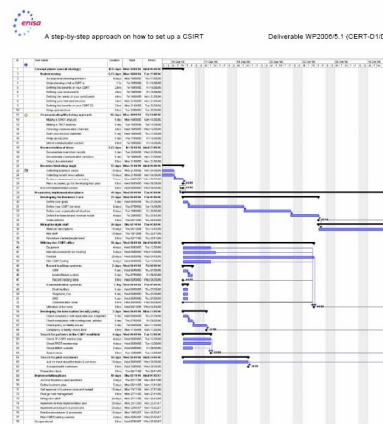
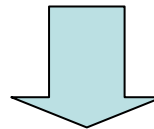
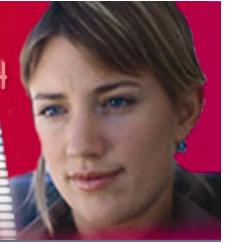


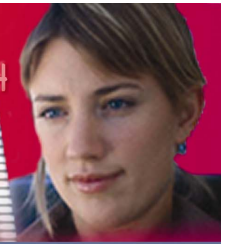
Fig. 18 The project plan with all tasks and a part of the Gant chart





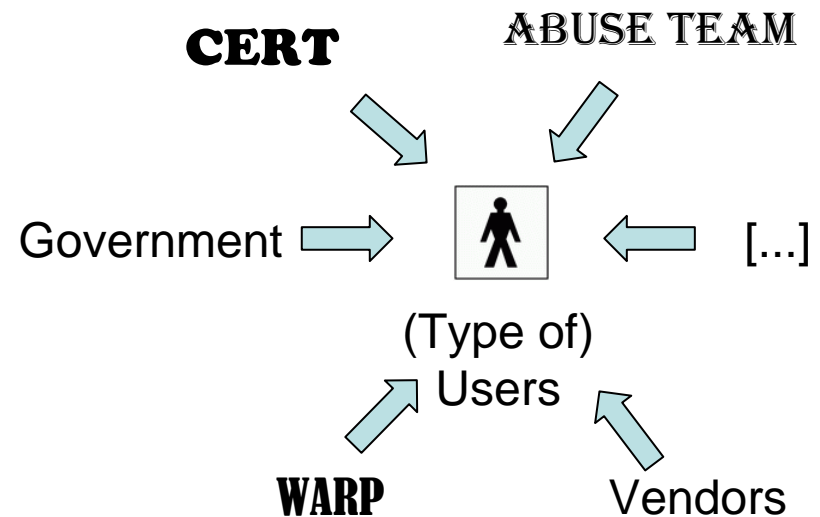
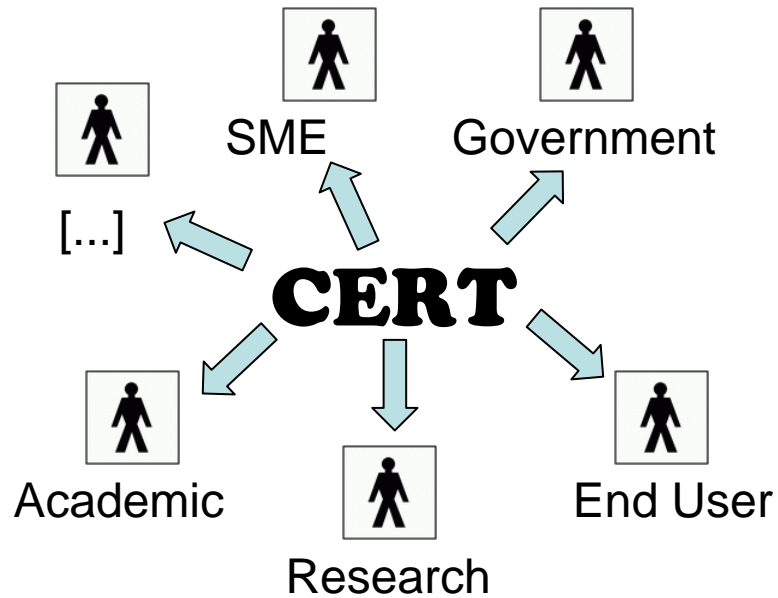
ENISA and CERTs 2007: Support existing teams

- 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

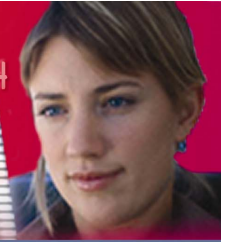
2007: Change focus (a bit)



Focus on CERT/CSIRT



Focus on the User (-groups)



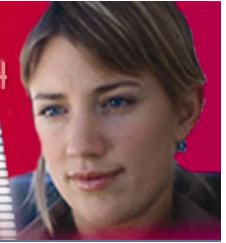
Ad-hoc Working-group 2006

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



Next events

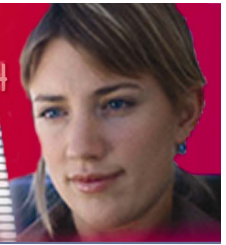
- Information Workshop in Brussels for the Member States 05.10.
- ISSE conference in Rome 10.-12.10. (PSG meeting)
- Workshop for newly built CSIRTs together with CERT PL 16.10.
- Secure 2006 conference in Warsaw together with CERT PL 17.-18.10.
- NCIRC workshop in Paris end of October
- Several other security related conferences (Lithuania, Malta, etc.)

Username:

Password:



5599 7774



Stay in touch with ENISA!

Go to our website:



<http://www.enisa.europa.eu>

Subscribe to our Quarterly Newsletter:

ENISA Quarterly



12/2005
[Download](#)
(PDF, 265 Kb)



10/2005
[Download](#)
(PDF, 265 Kb)



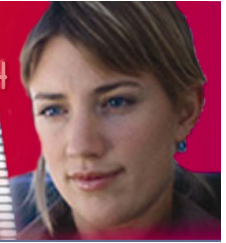
06/2005
[Download](#)
(PDF, 265 Kb)

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

Username:

Password:

5599 2774



Stay in touch with ENISA!



Visit us in Heraklion!

European Network and Information Security Agency

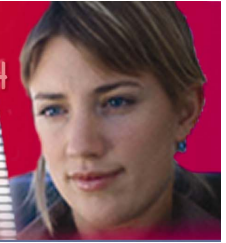
Science and Technology Park of Crete (ITE)

Vassilika Vouton,

70013 Heraklion, Greece

Meet us in Rome!





Thank You!

Questions?

Contact:

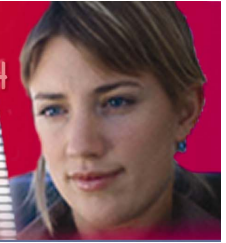
Marco THORBRUEGGE

Senior Expert Computer Security and Incident Response

Cooperation and Support Department

+30.2810.39.1372

marco.thorbruegge@enisa.europa.eu



Future of CHIHT?

CHIHT - Clearing House for Incident Handling Tools



This is a pilot site for a proposed collection of tools and guidelines of their use intended for incident handling teams. Information on this site reflects the experience of a number of European CSIRTs, working together as a project in the framework of the TERENA's Task Force [TF-CSIRT](#).

Disclaimer

Inclusion of a particular piece of software does not imply any form of recommendation from TERENA or the contributors. This is up to you to decide whether a particular program is suitable for your purposes.

Also note that an unauthorised use of some of these tools may constitute a criminal offence. Please read our [warning](#) before proceeding.

Clearinghouse Organisation

The first group of tools relates directly to the investigation of incidents. Tools are grouped by functions representing the normal sequence of an investigation.

- **Gathering evidence from the scene of an incident**
 - [Examining media](#)
 - [Examining system](#)
- **Investigating evidence of an incident**
 - [Analysing evidence](#)
 - [Checking identities](#)
- **Supportive tools for handling evidences**
- **Recovering the system after an incident**

The second group constitutes tools to support daily operations of CSIRT.

- **Implementing CSIRT operational procedures**
 - [Incident tracking and reporting](#)
 - [Incident archives](#)
 - [Communications](#)
- **Providing secure Remote access**
 - [Remote network access](#)
 - [Secure dial-up access](#)