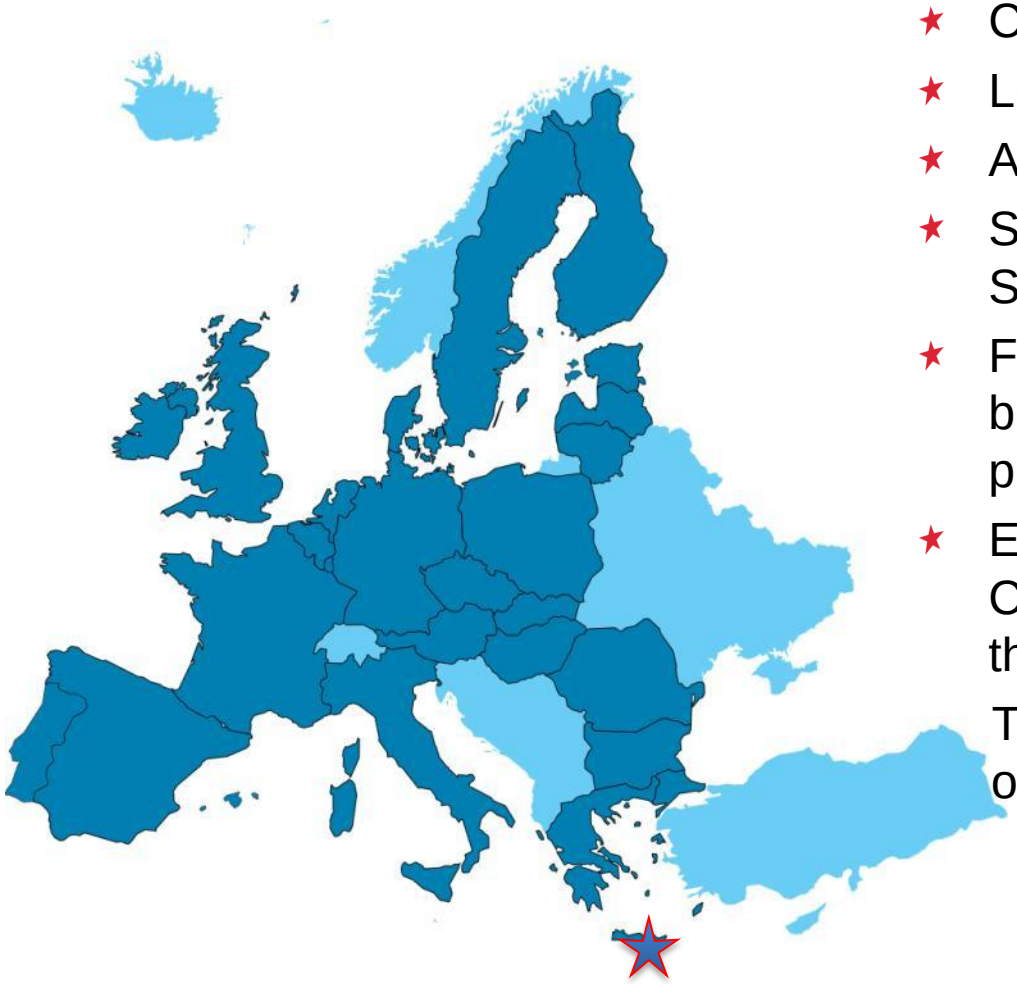
Securing Europe's Information Society

Dr. Udo Helmbrecht
Executive Director
European Network and Information Security Agency
16 June 2010 – FIRST AGM Miami

Agenda

- **ENISA overview**
- Challenges
- EU policy on NIS
- Overview of current activities
- Examples for current activities
- Outlook
- Conclusions

ENISA – overview



- Created in 2004
- Located in Heraklion / Greece
- Around 30 Experts
- Supports EU institutions and Member States
- Facilitator of information exchange between EU institutions, public sector & private sector
- ENISA assists Member States and the Commission in global issues that affect the European Community as a whole

This is an advisory role and the focus is on prevention and preparedness

Agenda

- ENISA overview
- **Challenges**
- EU policy on NIS
- Overview of current activities
- Examples for current activities
- Outlook
- Conclusions

NIS Challenges

- Complexity of global networks is increasing
- Number of security breaches is growing, leading to financial damage and undermining user confidence
- The economy of Europe is at stake if we do not manage security properly
- ICT systems are essential for economic and societal development
- We need to achieve a collaborative approach on increasing NIS to enable and enhance economic and societal development in priority areas, such as:
  - Improving Europe's critical information infrastructure protection (CIIP)
  - Enhancing Europe's early warning and incident response capabilities
  - Increasing user trust and confidence

NIS Challenges – cont.

- We need to achieve a collaborative approach on increasing NIS to enable and enhance economic and societal development in priority areas, such as:
  - Improving Europe's critical information infrastructure protection (CIIP)
  - Enhancing Europe's early warning and incident response capabilities
  - Increasing user trust and confidence

because

"Europeans will not embrace technology they do not trust - the digital age is neither "big brother" nor "cyber wild west"

(Digital Agenda for Europe, COM(2010) 245, 19.05.2010)

Agenda

- ENISA overview
- Challenges
- **EU policy on NIS**
- Overview of current activities
- Examples for current activities
- Outlook
- Conclusions

Network and Information Security (NIS)
The EU Policy Framework

2004: Establishment of the European Network and Information Security Agency - ENISA

2006: European Commission Strategy for a Secure Information Society - COM(2006)251

2007: Council Resolution on a Strategy for a Secure Information Society in Europe [2007/C 68/01]

2008: Extension of ENISA's mandate and launch of a debate on increased NIS

03/2009: European Commission's proposal for an Action Plan on Critical Information Infrastructure Protection - CIIP -

11/2009: Adoption of the revised telecoms regulatory package integrating provisions on security

12/2009: Council resolution on a collaborative European approach to NIS [2009/C 321/01]

05/2010: Commission's proposal for a modernized NIS Policy in the EU

The Digital Agenda

http://ec.europa.eu/information_society/digital-agenda/index_en.htm

DIGITAL AGENDA

- NIS “masterplan” for the next 10 years
- Proposes action areas for a European information society (like interoperability, standards, research, access and ...)

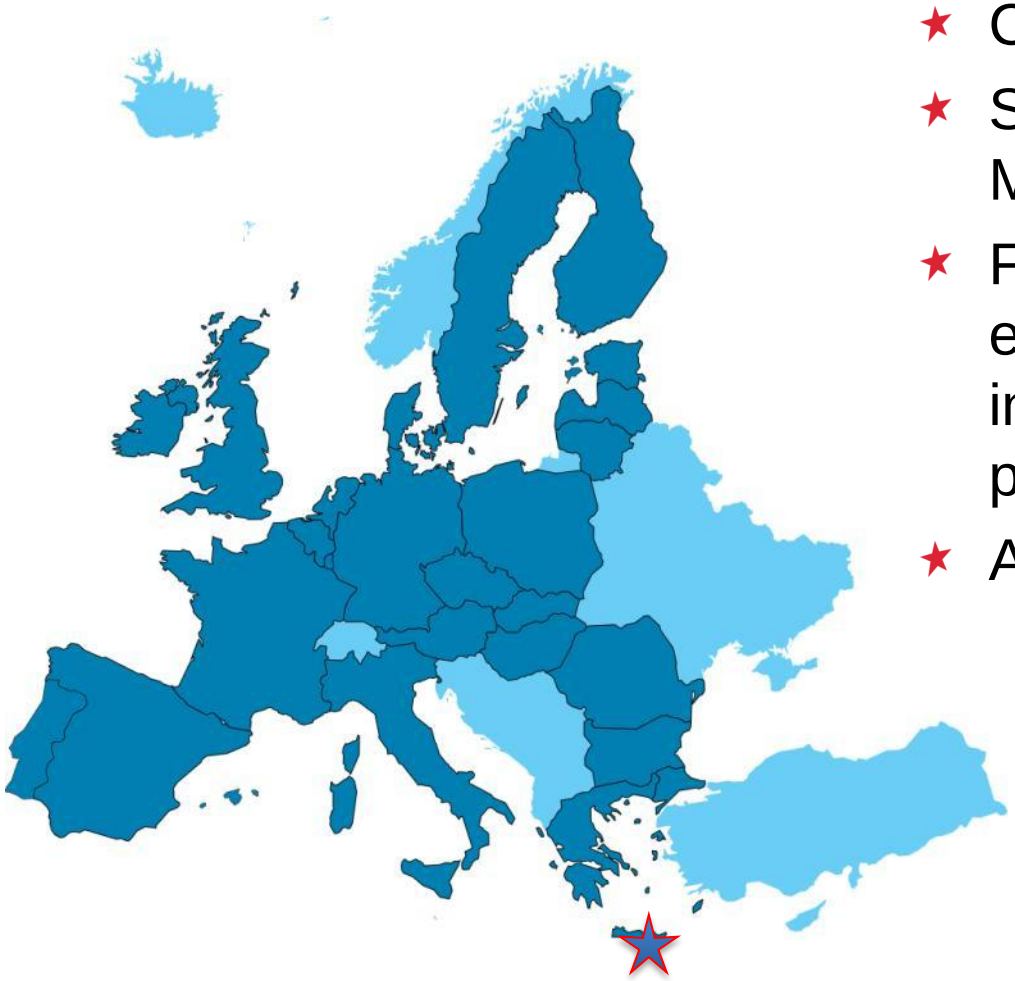
... Trust and security! High level goals:

- Modernise and enhance ENISA
- Enhance cooperation of CERTs on national and European level
- Provide CERT services for European institutions
- Support EU-wide cyber security preparedness exercises
- Enhance prevention and combating cybercrime

Agenda

- ENISA overview
- Challenges
- EU policy on NIS
- **Overview of current activities**
- Examples for current activities
- Outlook
- Conclusions

ENISA's Role in Europe



- Centre of Expertise
- Supports EU institutions and Member States
- Facilitator of information exchange between EU institutions, public sector & private sector
- Activities:
  - Advising and assisting
  - Collecting and analysing
  - Promoting methods
  - Raising awareness

ENISA's Mission

Securing Europe's Information Society by acting as a pacemaker for NIS

ENISA's Current Activities

- ENISA's work plan is based around a number of Multi-Annual Thematic Programs (MTPs)

- The current set of MTPs was launched in 2008. They cover the following areas:
  - Improving resilience in European networks
  - Developing and maintaining cooperation
  - Identifying emerging risks

- These MTPs are scheduled to finish in 2010

Improving resilience in European networks

- Goal : To improve Resilience in European eCommunications Networks & Services

- This work consists of three phases:
  - Stock-taking of regulatory/policy environments and provider measures
  - Identification of good practices and gap analysis
  - Support for deployment

- The scope of the work covers:
  - Policy issues
  - Deployment issues
  - Technical issues (e.g. DNSSEC)

Cross-border cooperation

- Goal : To increase cooperation between Member States to reduce differences in capability between Member States in the area of NIS
- ENISA develops and supports cooperation models in pre-defined areas
- Currently, these areas are:
  - Awareness Raising
  - Reinforcing national / gov. CERTs
  - European NIS good practice brokerage

Emerging Risks

- Goal: To enable stakeholders to better identify and understand Emerging and Future Risks in the area of NIS
- Scenarios submitted by public sector and private sector stakeholders
- Expert groups are used to validate and analyse submitted scenarios from a risk standpoint
- Will be supplemented by the creation of a Knowledge Base

Agenda

- ENISA overview
- Challenges
- EU policy on NIS
- Overview of current activities
- **Examples for current activities**
- Outlook
- Conclusions

Activity example: Reinforcing national/governmental CERTs

The objectives are:

- Definition and further development of a set of baseline capabilities for national / governmental CERTs in the Member States
- Establish national / governmental CERTs in every Member State
- Offer or support activities to help teams to reach (and go beyond) the baseline

- Enhance cooperation on national and European level

Activity example: Reinforcing national/governmental CERTs

Means

- *Support setting up*
- *Training*
- *Exercises*

Support in

- *Reaching out to (new) constituencies (EISAS)*
- *Enhancing existing services*
- *Extension of services*
- *Information sharing and cooperation*
- *Etc.*

Activity example: Reinforcing national/governmental CERTs

2005: Stocktaking

2006: Setting up & Cooperation

2007: Support Operation Quality Assurance

2008: CERT Exercises

2009: CERT Exercises Pilots

2010: CERT Baseline Capabilities

TERENA

TRUSTED Introducer

NCIRC NATO COMPUTER INCIDENT RESPONSE CAPABILITY

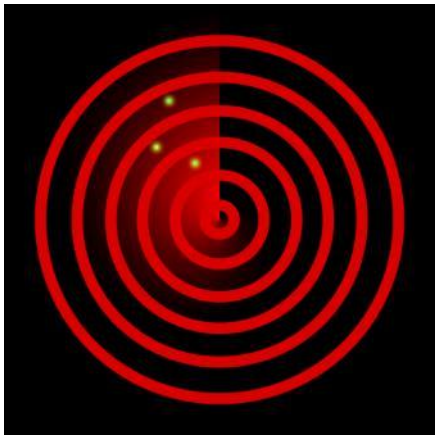
FIRST Improving Security Together

APCERT Asia Pacific Computer Emergency Response Team

[...]

Activity example: National and pan-European exercises

The objectives are:



- First pan-European exercise in 2010
- Collaborate with EuroCybex towards preparing an advanced exercise in 2011
- Support the implementation of the Good Practice Guide on National Preparedness Exercises by Member States
- Develop a robust framework for running Pan European (and multinational in general) exercises with long term strategic objectives

Activity example: Awareness Raising

- Enhance information exchange on awareness raising among national / governmental level organisations
- Establish a task force for information security awareness within the EU institutions and bodies.
- Continue to address the challenges of young generation and family online safety.
- Continue to build the AR Community
- Support the Commission and Member States in establishing a European Security week.

Activity example: Cloud Computing for governments

- In 2009, ENISA published the cloud computing risk assessment and cloud assurance framework
- In 2010, ENISA is performing an analysis of Government Cloud initiatives from the security and resilience perspective
- In 2011 this will be followed up with an initiative which pilots the use of these criteria within EuropeanGovernment procurement criteria
- Conference on cloud assurance in Q2 2011
- Pilot study with member states, by Q4 2011

Agenda

- ENISA overview
- Challenges
- EU policy on NIS
- Overview of current activities
- Examples for current activities
- **Outlook**
- Conclusions

Outlook 2011:
Situation awareness for CERTs

The objectives are:

- Stock taking of available situation awareness mechanisms to define the “state of the art” of “early warning” for NIS.

- Analysis of results - the benefits and shortcomings will be assessed and potential further developments identified.

Outlook 2011:
Cross-border CERT cooperation

The objectives are:

- Examine barriers and incentives for cross-border collaboration and information sharing (i.e. legal issues, data protection, etc.)
- Examine “operational gaps on European level”
- Examine “operational redundancies and synergies”

Agenda

- ENISA overview
- Challenges
- EU policy on NIS
- Overview of current activities
- Examples for current activities
- Outlook
- **Conclusions**

Our Vision

- Everybody is involved.
  - All actors understand the role they are expected to play and are sufficiently knowledgeable to perform this role.
- Actions performed by the different actors are mutually reinforcing.
  - This is the principle of defence in depth.
- The approach is sufficiently scalable and flexible to cope with rapidly evolving constraints.
  - Approaches that are too rigid and that cannot adapt to changes in the socio-economic environment will not survive.

Conclusions

- We need to move towards a situation in which all actors recognise and proactively manage risks.
- Methods and tools should be flexible and scalable. They should be capable of delivering tangible results with reasonable investment.
- Infrastructure should offer true end-to-end security.
- By closely following emerging risks, aligning research with these risks, and deploying research results faster, we will be able to securely leverage new technologies earlier.
- New concepts need to be quickly understood and leveraged to improve current security models.
- Achieving coherence and consistency over time will be a major challenge.

Contact

European Network and Information Security Agency

Science and Technology Park of Crete (ITE)
P.O. Box 1309
71001 Heraklion - Crete – Greece

cert-relations@enisa.europa.eu
http://www.enisa.europa.eu