ENISA & Cybersecurity

Steve Purser
Head of Technical Competence Department
December 2012

Agenda

- Protecting Critical Information Infrastructure
- Input to EU & MS Cyber Security Strategies
- Assisting Operational Communities
- Security & Data Breach Notification
- Data Protection

Cyber Exercises

- Cyber Europe 2010.
  - Europe's first ever international cyber security exercise
- EU-US exercise, 2011.
  - Also a first : work with COM & MS to build transatlantic cooperation
- Cyber Europe 2012.
  - Developed from 2010 & 2011 exercises.
  - Involves MS, private sector and EU institutions.
  - Highly realistic exercise, Oct 2012

EFMS & EP3R

- The European Forum for Member States builds on national approaches to CIIP.
  - It will be used to foster common understanding of the issues and strategies for dealing with them.
- The European PPP for Resilience will provide a framework for supporting collaboration between public and private sectors on NIS policy issues.
- ENISA is supporting both these initiatives:
  - Ensuring exchange of expertise on policy and operational aspects.
  - Provision of good practice guides.
  - Identifying significant risks and proposing suitable mitigation strategies.

www.enisa.europa.eu

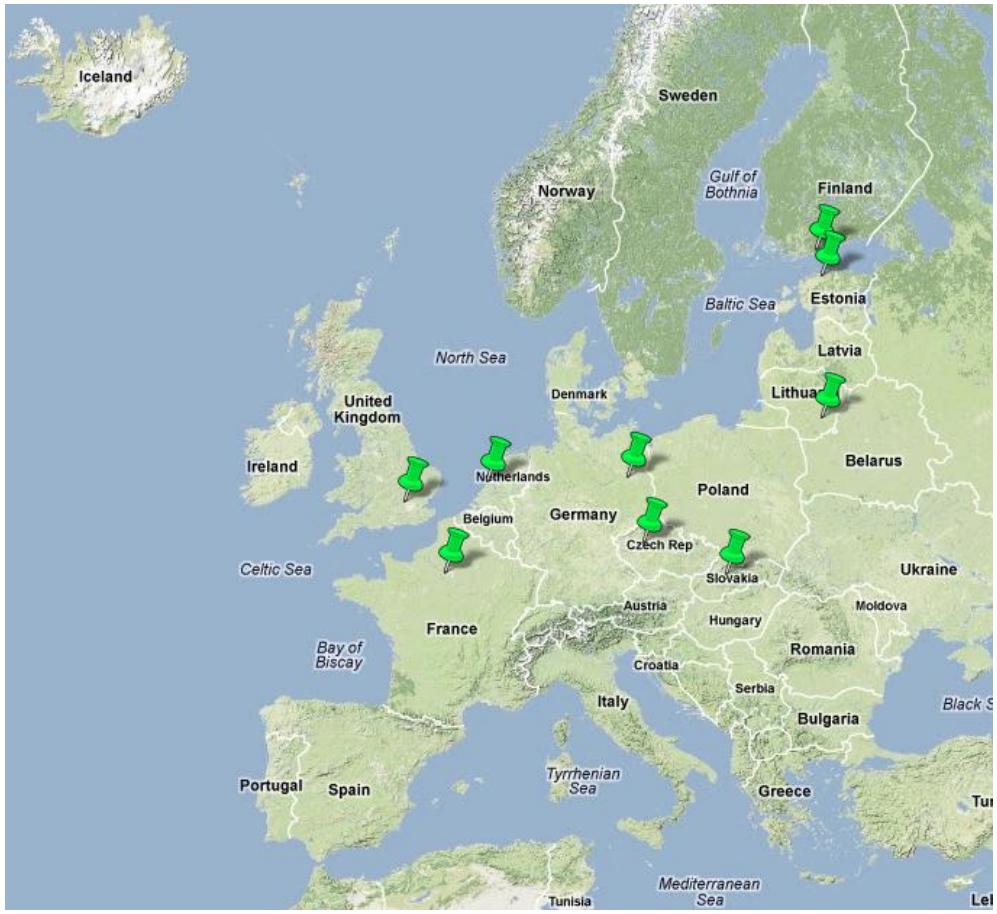
Securing New Technologies

Agenda

- Protecting Critical Information Infrastructure
- Input to EU & MS Cyber Security Strategies
- Assisting Operational Communities
- Security & Data Breach Notification
- Data Protection

Member States with NCSS

- ✓ Czech Republic
- ✓ Estonia
- ✓ Finland
- ✓ France
- ✓ Germany
- ✓ Lithuania
- ✓ Luxemburg
- ✓ Netherlands
- ✓ Slovakia
- ✓ United Kingdom



Good Practice Guide

- ENISA project for 2012 (delivery Q4)
- Will describe
  - Known good practices, standards and policies
  - The elements of a good Cyber Security Strategy
  - Institutions and roles identified in a Strategy
  - Parties involved in the development lifecycle
  - Challenges in developing and maintaining a Strategy

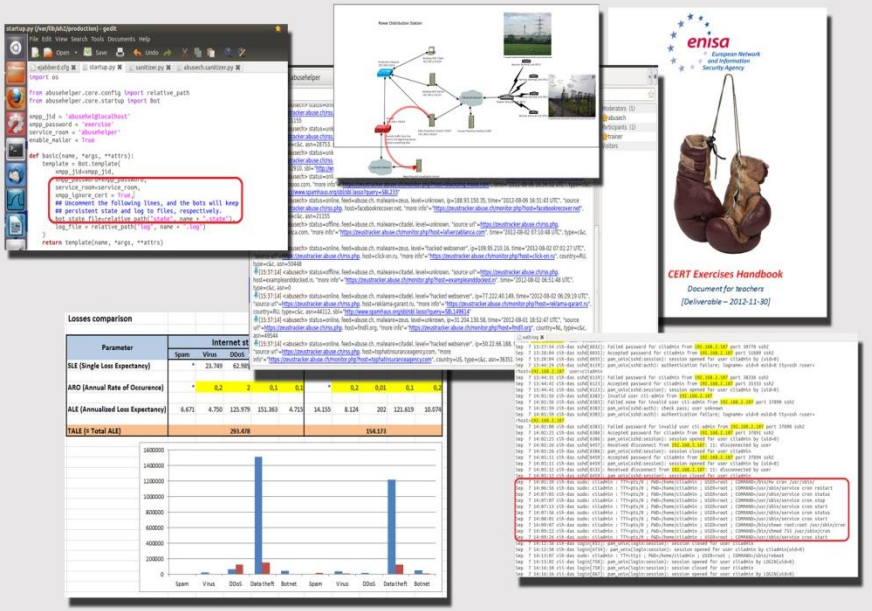
Agenda

- Protecting Critical Information Infrastructure
- Input to EU & MS Cyber Security Strategies
- Assisting Operational Communities
- Security & Data Breach Notification
- Data Protection

Supporting Operational Communities - Overview

Supporting the CERT community

ENISA Annual **CERT workshops**
focus on national and governmental CERTs preparedness and response capabilities



New Exercise material 2012
- Technical trainings for CERTs
- Handbook for teachers
- Toolset for students
- SW ready to use from our website:
www.enisa.europa.eu/activities/cert/support

FIRST – to improve CERT capabilities

TRANSITS framework: support the basic and advanced training courses for CERTs

Cross-communities Support

INTERPOL
Atomic exercise 2012

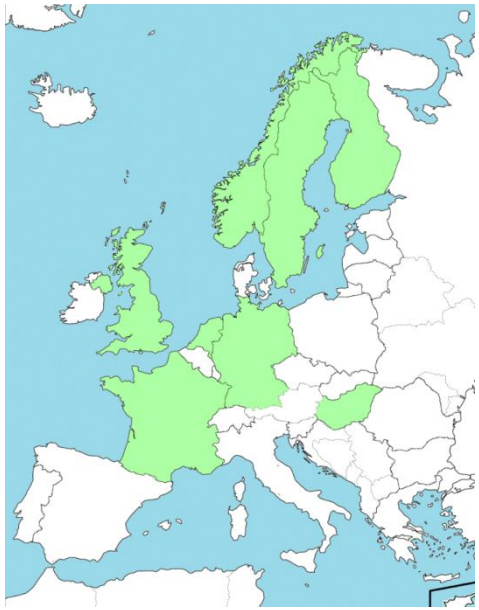
ENISA-EUROPOL joint workshop:
"Addressing NIS aspects of cybercrime"

EU FI-ISAC exercise for CERTs, LEA and banks

CEPOL courses: (operational security unit supports cyber work-shops for police)

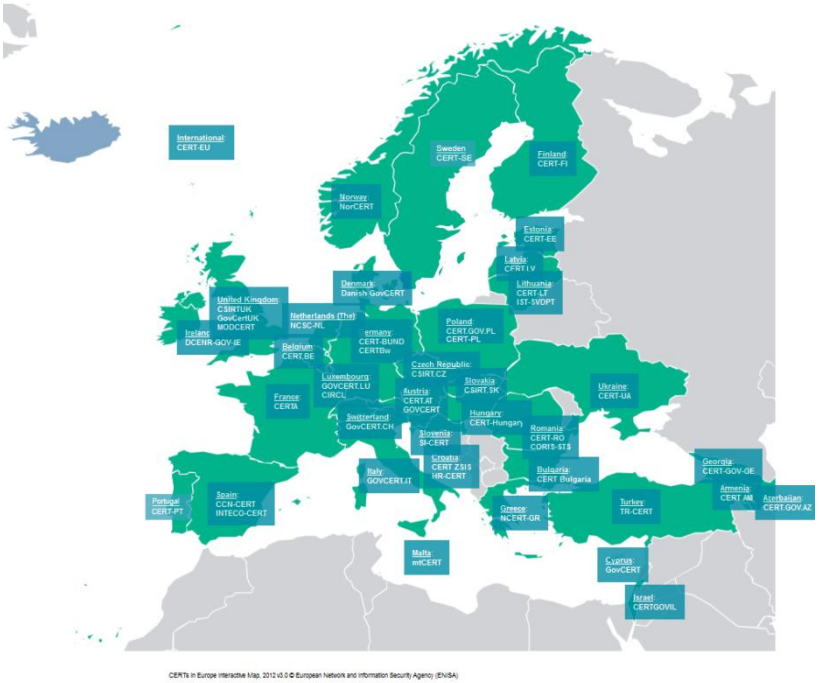
National/governmental CERTs the situation has changed…

in 2005



ESTABLISHED IN 2005:
Finland
France
Germany
Hungary
The Netherlands
Norway
Sweden
UK

in 2012



CERTs in Europe interactive Map, 2012 v3.0 © European Network and Information Security Agency (ENISA)

Baseline capabilities of n/g CERTs

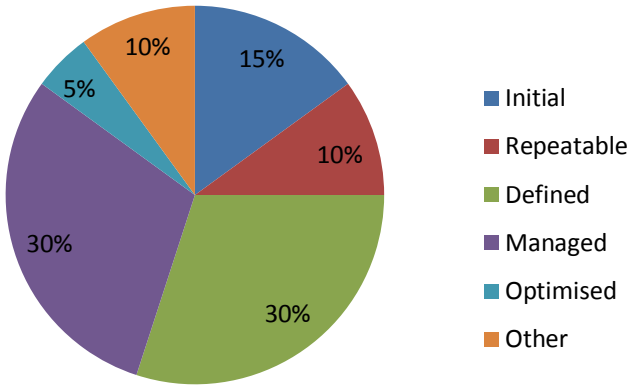
- Initially defined in 2009 (operational aspects)
- In 2010 Policy recommendations drafted
- In 2012 ENISA continues to work on a harmonisation together with MS

- Status Report 2012
- National/governmental CERT capabilities – updated recommendations 2012

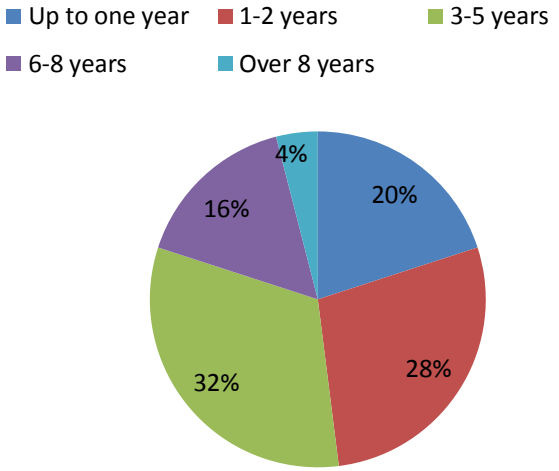
CERT Status Report 2012

Total: 45 responses to the questionnaire (25 from n/g CERTs; 20 from other CERTs and other stakeholders)

Self-Assessment of the Maturity Status of National / Governmental CERTs



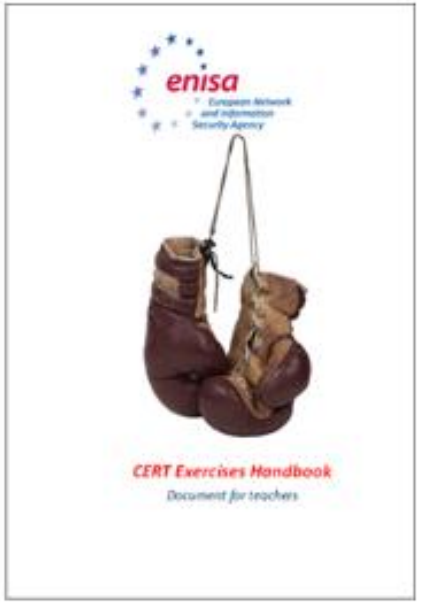
Years of Operation of National / Governmental CERT



Interviewed teams assessed themselves as either governmental or national/governmental CERTs indicated the years of operations between: 4 months and 11 years.
(France, Germany, Norway, Hungary, Denmark, Sweden, Spain, Ireland, Latvia, Czech Republic, Slovakia, Romania, CERT-EU)

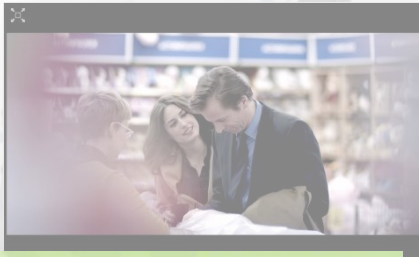
CERT Exercises and training material

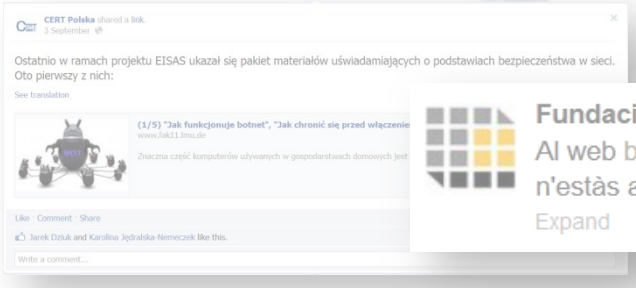
- ENISA CERT training/exercise material, used since 2009, was extended to host 23 different topics and training exercises including:
  - Technical aspects
  - Organisational aspects
  - Operational aspects
- Additionally a Roadmap was created to answer the question ‘How could ENISA provide more proactive and efficient CERT training?



EISAS – Large Scale Pilot

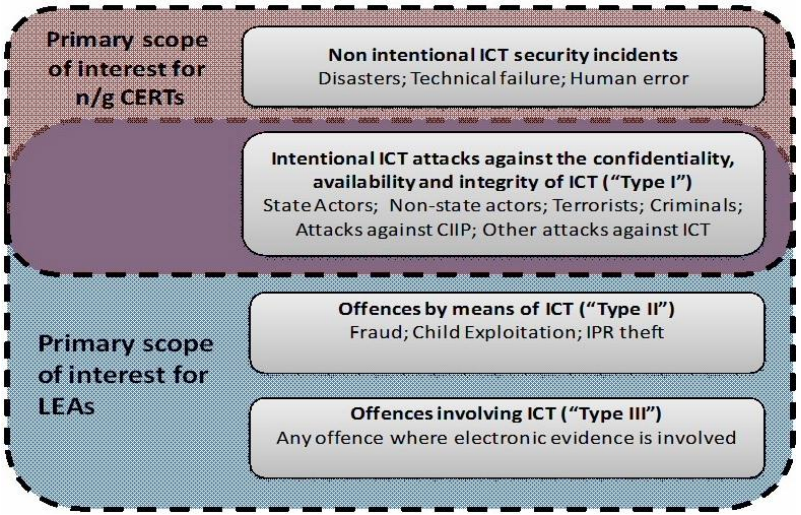
- European Information Sharing and Alert System introduced in COM(2006) 251: “Communication on a strategy for a Secure Information Society”
- In 2012: Pilot Project for collaborative Awareness Raising for EU Citizens and SMEs
  - Gathered n/g CERTs, governmental agencies and private companies in 6 different MS
  - Cross-border awareness raising campaign
  - Reached more than 1.700 people in 5 months
  - Social networks involved





Fostering CERT-LEA Collaboration

- Main goals:
  - Define key concepts
  - Describe the technical and legal/regulatory aspects of the fight against cybercrime
  - Compile an inventory of operational, legal/regulatory and procedural barriers and challenges and possible ways to overcome these challenges
  - Collect existing good and best practices
  - Develop recommendations
- Focus on CERT-LEA cooperation



Agenda

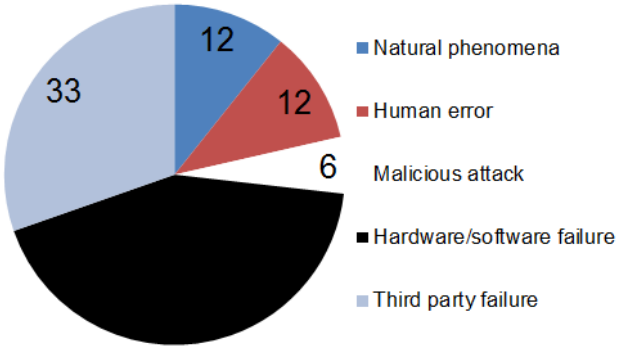
- Protecting Critical Information Infrastructure
- Input to EU & MS Cyber Security Strategies
- Assisting Operational Communities
- Security & Data Breach Notification
- Data Protection

Security & Data Breach Notification

- Supporting MS in implementing Article 13a of the Telecommunications Framework Directive
  - Supported NRA's in implementing the provisions under article 13a
  - Developed and implemented the process for collecting annual national reports of security breaches
  - Developed minimum security requirements and propose associated metrics and thresholds
- Supporting COM and MS in defining technical implementation measures for Article 4 of the ePrivacy Directive.
  - Recommendations for the implementation of Article 4.
  - Collaboration with Art.29 TS in producing a severity methodology for the assessment of breaches by DPAs

Article 13a - Incidents 2011

- 51 incidents from 11 countries, 9 countries without significant incidents, 9 countries with incomplete implementation
- Most incidents
  - Affect mobile comms (60%)
  - Are caused by
    - hardware/software failures (47%)
    - third party failures (33%),
    - natural disasters (12%)
  - Many involve power cuts (20%)
  - Natural disasters (storm, floods, et cetera)
    - often cause power cuts, which cause outages



Severity of a data breach

Estimation of the magnitude of potential impacts on the individuals' privacy and data protection

Low	Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Data subjects may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
Very High	Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

Agenda

- Protecting Critical Information Infrastructure
- Input to EU & MS Cyber Security Strategies
- Assisting Operational Communities
- Security & Data Breach Notification
- Data Protection

‘The right to be forgotten’ – *between expectations and practice*

- Included in the proposed regulation on data protection published by the EC in Jan 2012.
- ENISA addressed the technical means of assisting the enforcement of the right to be forgotten.
- A purely technical and comprehensive solution to enforce the right in the open Internet is generally not possible.
- Technologies do exist that minimize the amount of personal data collected and stored online.