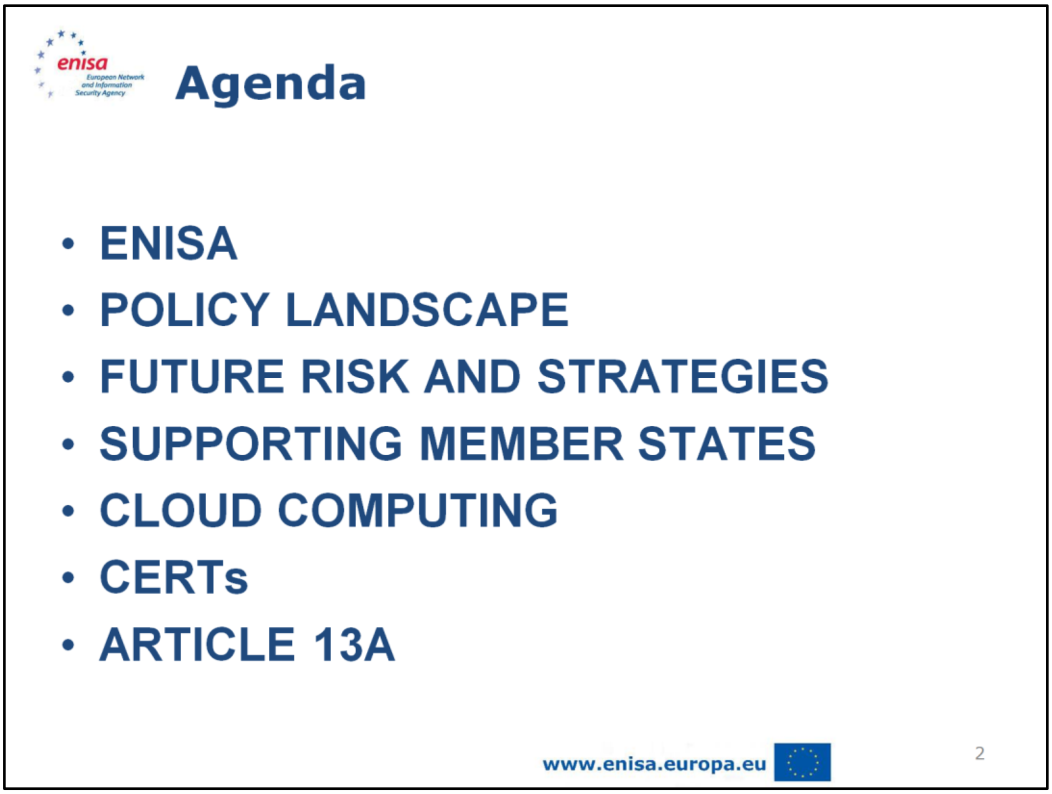
enisa
European Network and Information Security Agency

Global challenges in IT security
An EU perspective

Udo Helmbrecht
Executive Director, ENISA

Münchner Kreis, Fachkonferenz
Munich, 29th March 2012

www.enisa.europa.eu



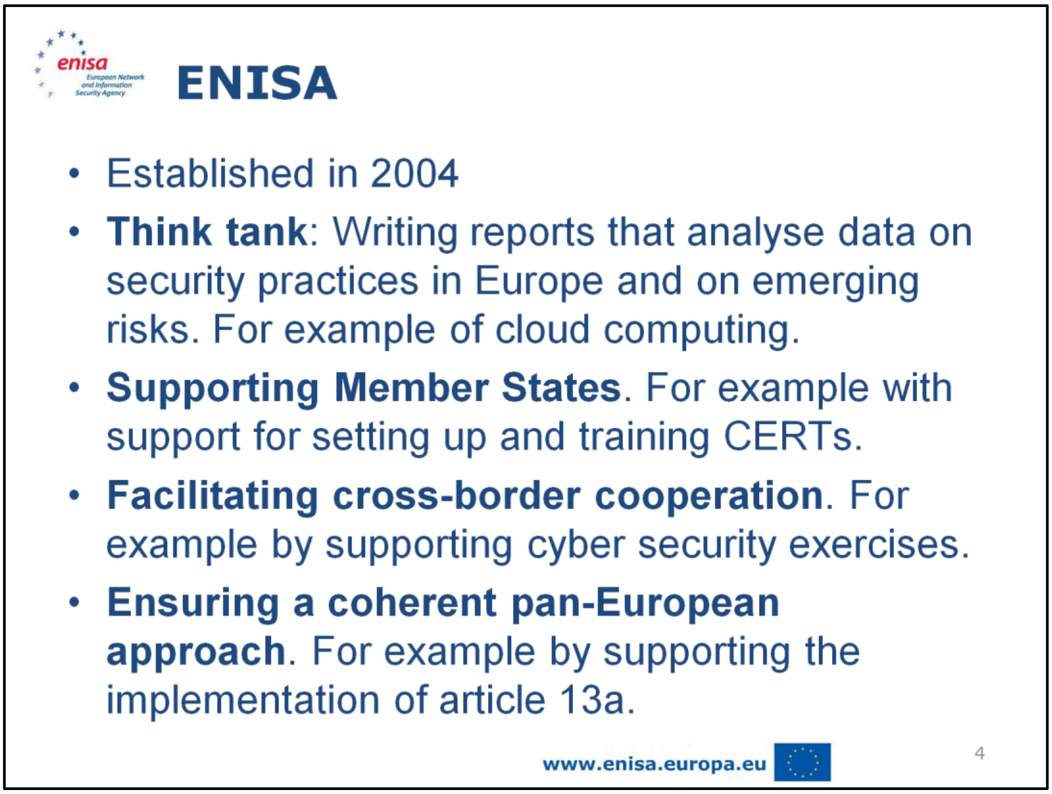
Agenda

- ENISA
- POLICY LANDSCAPE
- FUTURE RISK AND STRATEGIES
- SUPPORTING MEMBER STATES
- CLOUD COMPUTING
- CERTs
- ARTICLE 13A

www.enisa.europa.eu

2

ENISA



ENISA

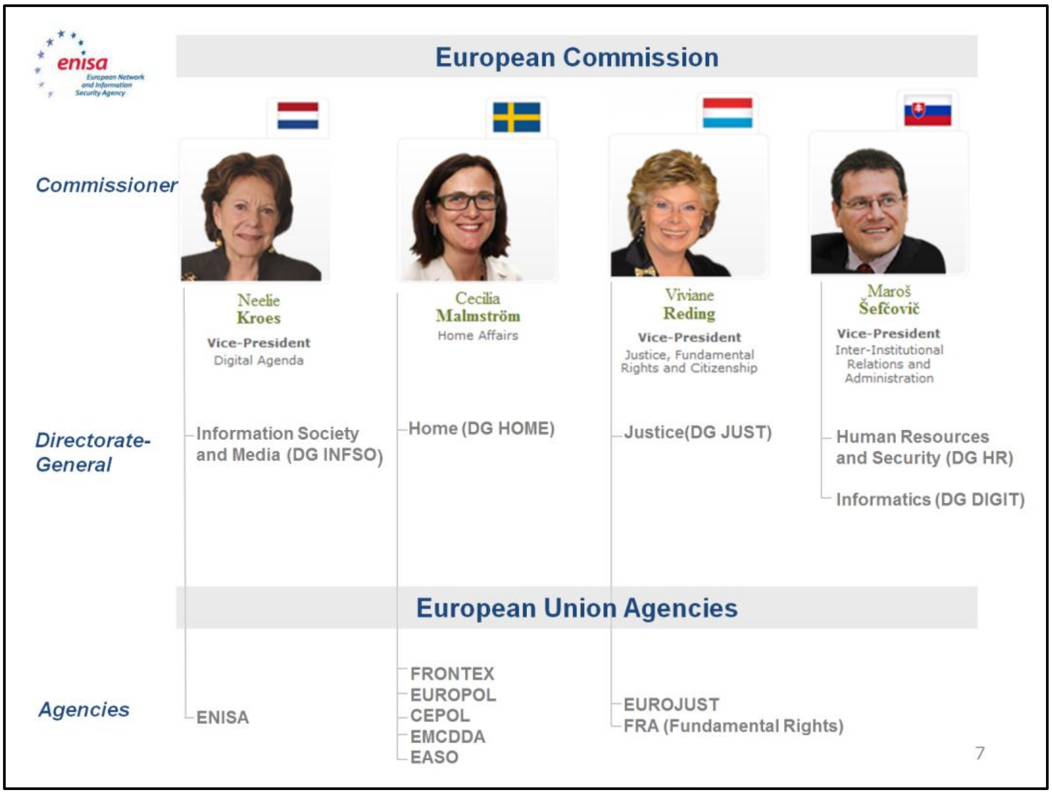
- Established in 2004
- **Think tank**: Writing reports that analyse data on security practices in Europe and on emerging risks. For example of cloud computing.
- **Supporting Member States**. For example with support for setting up and training CERTs.
- **Facilitating cross-border cooperation**. For example by supporting cyber security exercises.
- **Ensuring a coherent pan-European approach**. For example by supporting the implementation of article 13a.

POLICY LANDSCAPE

enisa
European Network and Information Security Agency

500 million people in 27 MS

www.european-council.europa.eu
www.consilium.europa.eu
European Union
Belgium
Bulgaria
Czech Republic
Denmark
Germany
Estonia
Ireland
Greece
Spain
France
Italy
Cyprus
Latvia
Lithuania
Luxembourg
Hungary
Malta
Netherlands
Austria
Poland
Portugal
Romania
Slovenia
Slovakia
Finland
Sweden
United Kingdom
BARENTS SEA
WHITE SEA
SEA OF NORWAY
SWEDEN
FINLAND
NORTH SEA
ATLANTIC OCEAN
IRELAND
UNITED KINGDOM
DENMARK
BALTIC SEA
ESTONIA
LATVIA
LITHUANIA
THE NETHERLANDS
BELGIUM
GERMANY
POLAND
CZECH REPUBLIC
SLOVAKIA
AUSTRIA
HUNGARY
ROMANIA
FRANCE
SLOVENIA
ITALY
BULGARIA
PORTUGAL
SPAIN
GREECE
BLACK SEA
MEDITERRANEAN SEA
TYRRHENIAN SEA
IONIAN SEA
MALTA
CYPRUS



enisa
European Network and Information Security Agency

European Commission

Commissioner

Neelie Kroes
Vice-President
Digital Agenda

Cecilia Malmström
Home Affairs

Viviane Reding
Vice-President
Justice, Fundamental Rights and Citizenship

Maroš Šefčovič
Vice-President
Inter-Institutional Relations and Administration

Directorate-General

- Information Society and Media (DG INFSO)
- Home (DG HOME)
- Justice(DG JUST)
- Human Resources and Security (DG HR)
- Informatics (DG DIGIT)

European Union Agencies

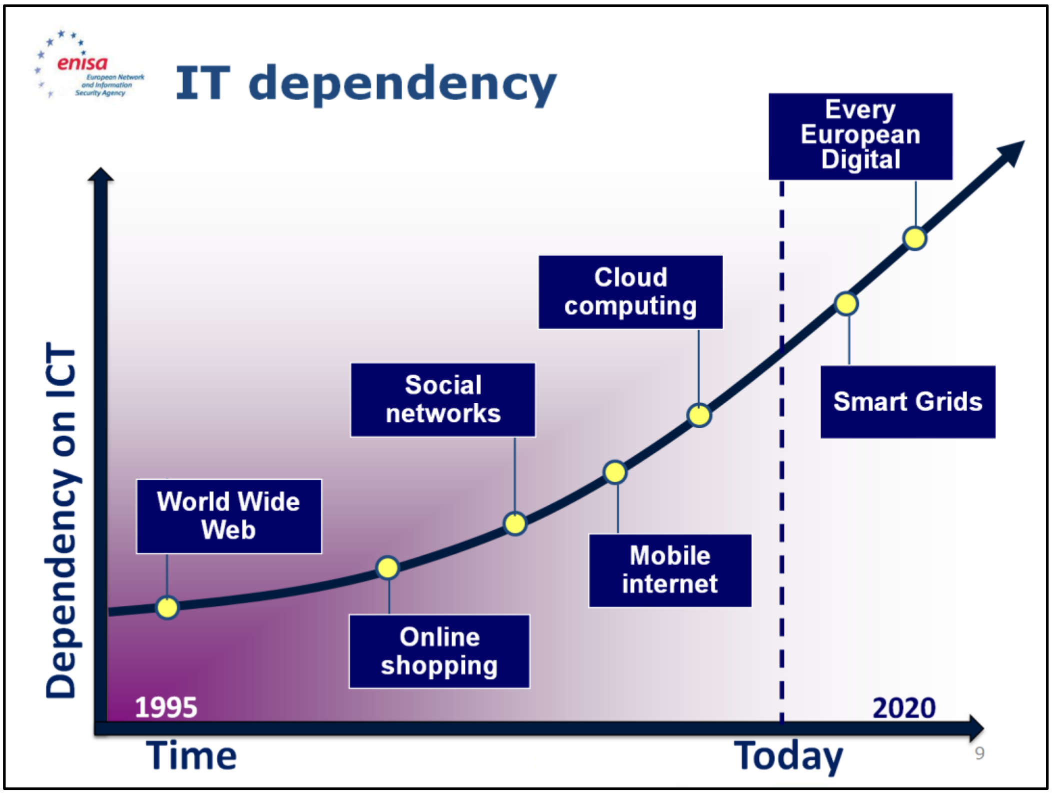
Agencies

- ENISA
- FRONTEX
- EUROPOL
- CEPOL
- EMCDDA
- EASO
- EUROJUST
- FRA (Fundamental Rights)

7

The Commission is divided into 33 ‘departments’. The departments are known as Directorates-General (DGs). NIS issues touch upon many of these.
EMCDDA = European Monitoring Centre for Drugs and Drug Addiction
EASO = European Asylum Support Office

FUTURE RISKS AND STRATEGIES



enisa
European Network and Information Security Agency

IT dependency

Dependency on ICT

World Wide Web

Online shopping

Social networks

Mobile internet

Cloud computing

Smart Grids

Every European Digital

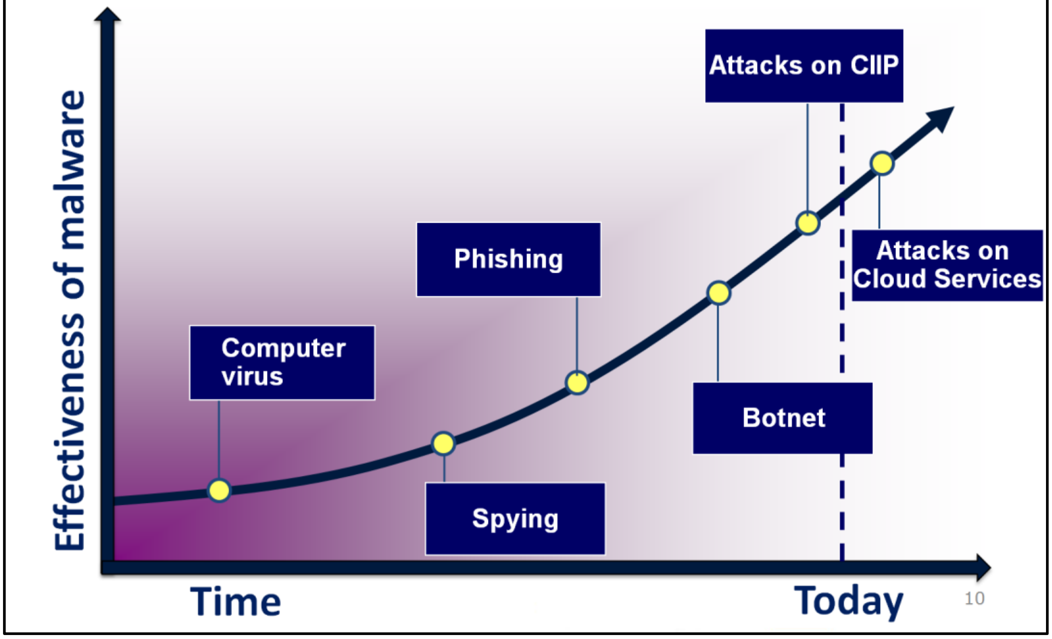
1995

2020

Time

Today

Development of attacks

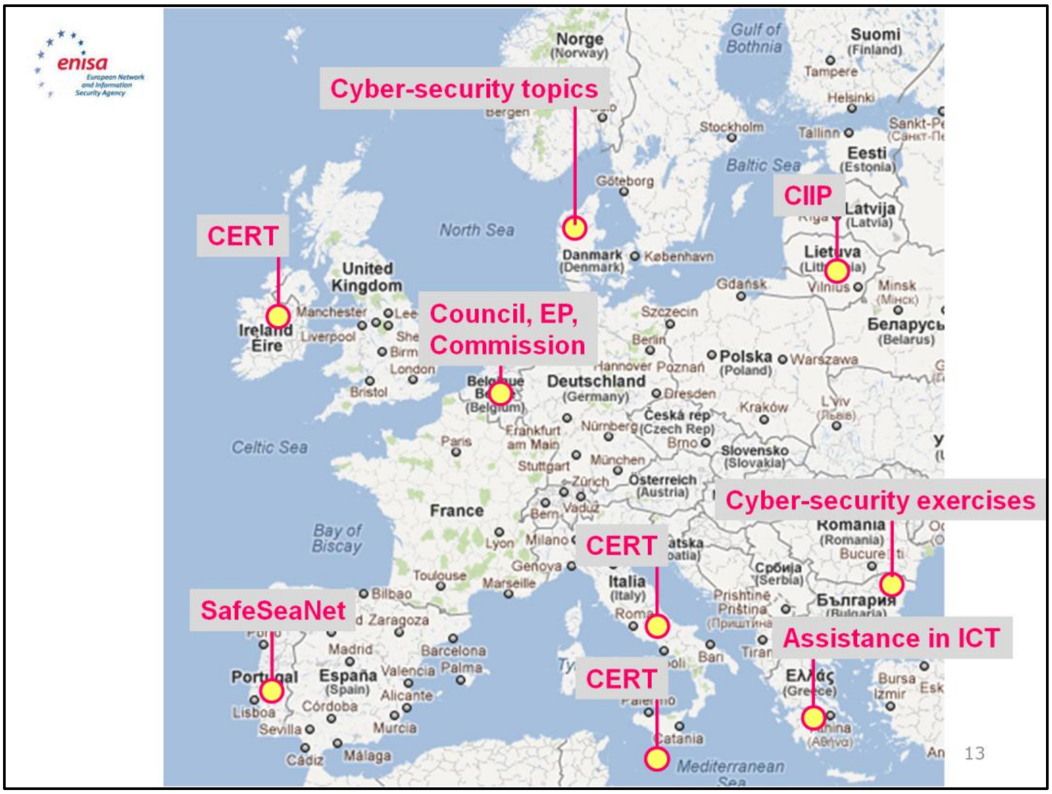


10

New virtual world

- No national borders
- No uniform legal system
- A new currency: personal data

SUPPORTING MEMBER STATES


enisa
European Network and Information Security Agency
Cyber-security topics
CERT
CIIP
Council, EP, Commission
Cyber-security exercises
CERT
SafeSeaNet
Assistance in ICT
CERT
13

CLOUD COMPUTING

Cloud computing

2009: Risk analysis

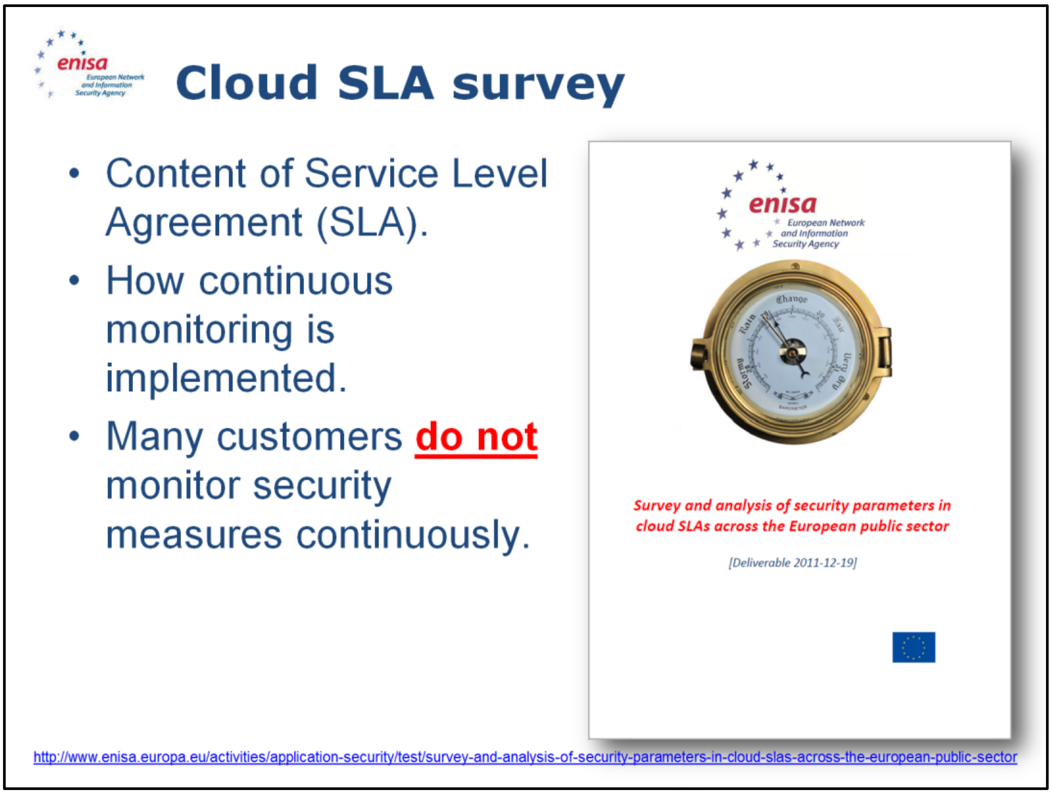
2009: Assurance framework

2011: Security and resilience in governmental clouds

2011: Security parameters in cloud SLAs

www.enisa.europa.eu

15



Cloud SLA survey

- Content of Service Level Agreement (SLA).
- How continuous monitoring is implemented.
- Many customers **do not** monitor security measures continuously.

enisa
European Network and Information Security Agency

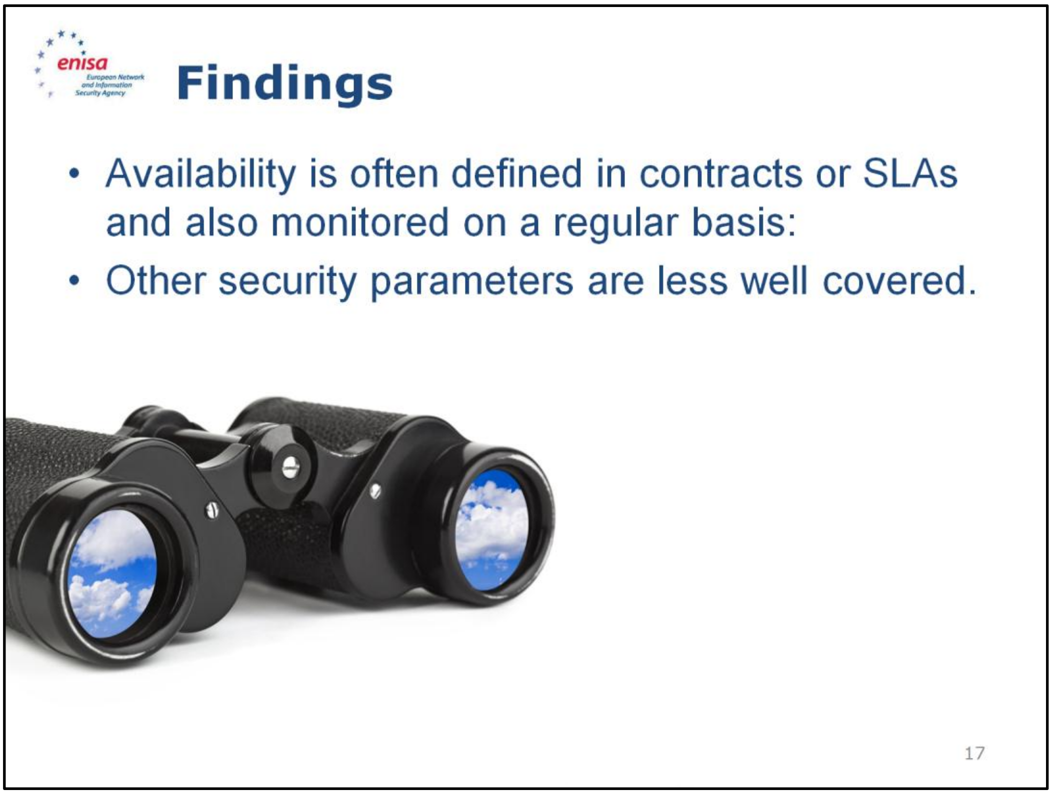
Survey and analysis of security parameters in cloud SLAs across the European public sector

[Deliverable 2011-12-19]

http://www.enisa.europa.eu/activities/application-security/test/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector

- Focuses on what is measurable in the contract: the Service Level Agreement (SLA) and how continuous monitoring is implemented.
- Draws attention to the fact that many customers do not monitor security measures continuously. This means that customers are in the dark about many important security aspects of their services. The risk is that they find out about failing security measures when it is already too late.

- Draws attention to the fact that many customers do not monitor security measures continuously. This means that customers are in the dark about many important security aspects of their services. The risk is that they find out about failing security measures when it is already too late.



Findings

- Availability is often defined in contracts or SLAs and also monitored on a regular basis:
- Other security parameters are less well covered.

17

Availability is often defined in contracts or SLAs and also monitored on a regular basis:

- 75% of the contracts define availability requirements.
- 50% of the contracts stipulate that availability be measured regularly.
- In 78% of the cases the provider is obliged to report service outages.

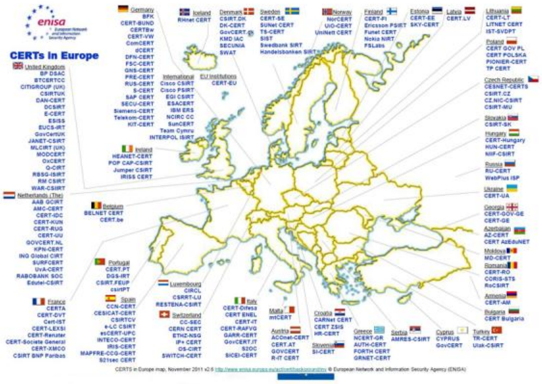
Other security parameters are less well covered:

- Only 32% of contracts include a classification of security incidents.
- In 57% of the cases penetration tests have been performed at some point, but only in 16% of the case penetration tests were performed regularly.
- Data portability is tested regularly in only 12% of the cases.
- Only 50% require load testing after first use
- Failover and backup tests are carried out regularly only in 26% of the cases.

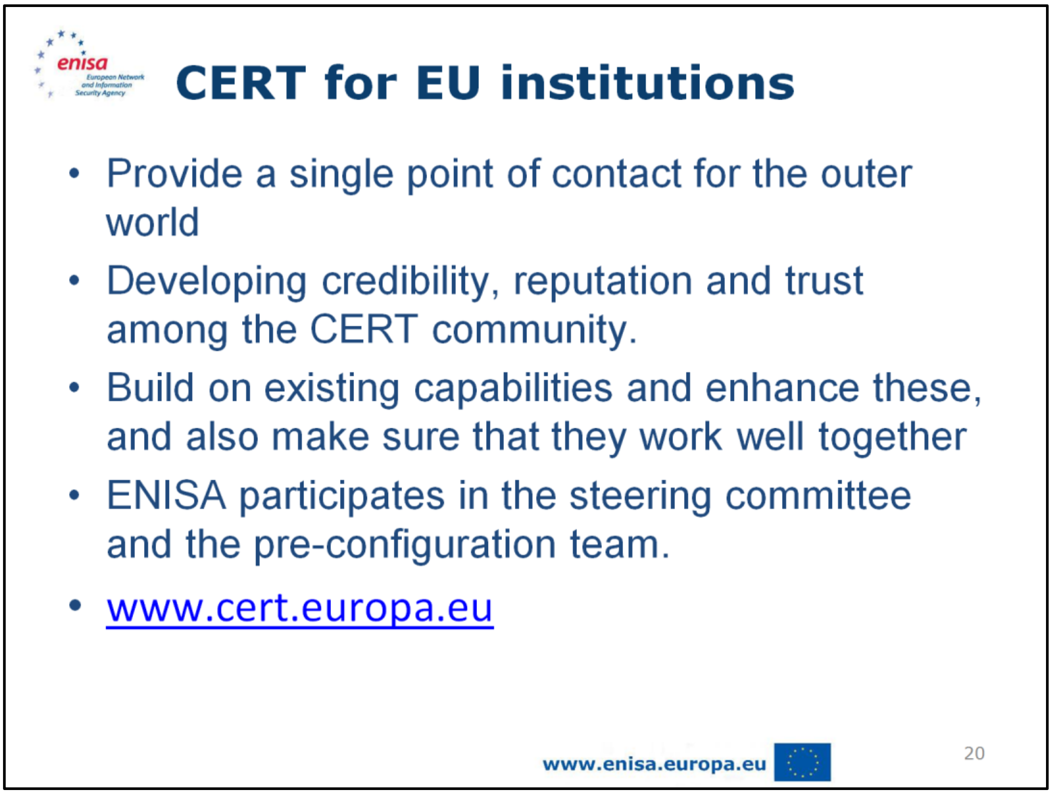
CERTS

CERTs at ENISA

- Support MS in establishing and developing CERTs to a baseline set of capabilities.
- Providing good practice in cooperation with CERTs.
- Analyse barriers for cross-border cooperation.
- Support cooperation between CERTs and crucial stakeholders.

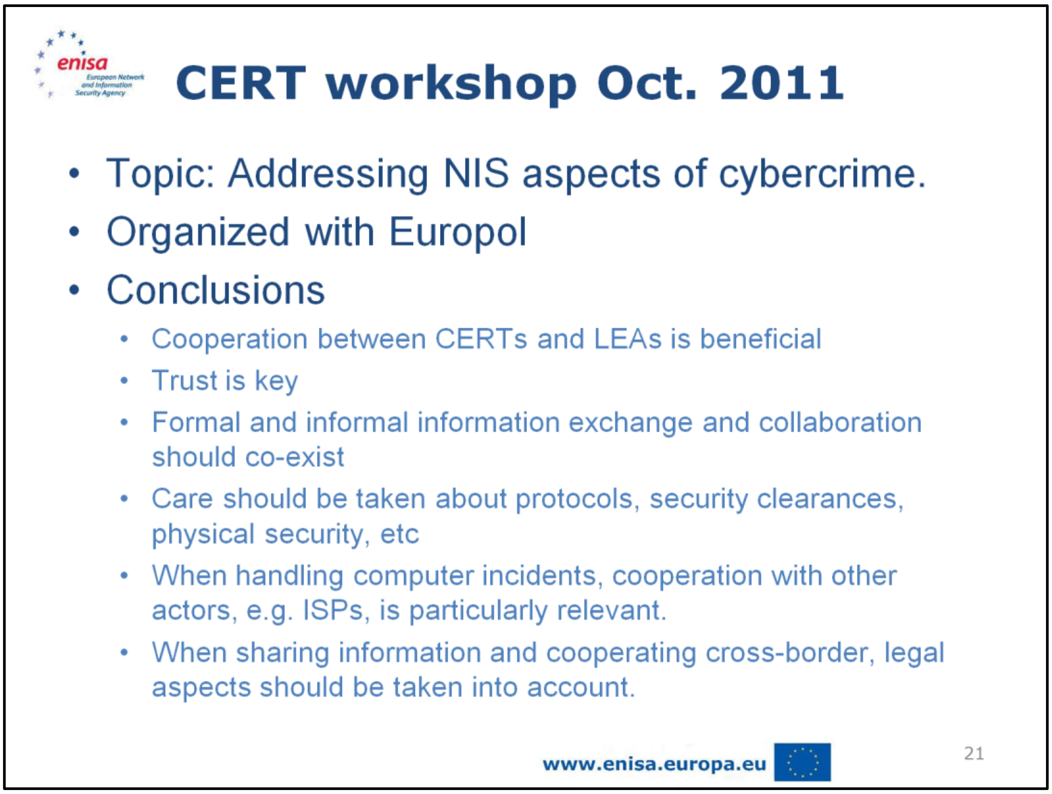


CERTS in Europe map, November 2011 v2.6 http://www.enisa.europa.eu/act/cert/background/inv © European Network and Information Security Agency (ENISA)



CERT for EU institutions

- Provide a single point of contact for the outer world
- Developing credibility, reputation and trust among the CERT community.
- Build on existing capabilities and enhance these, and also make sure that they work well together
- ENISA participates in the steering committee and the pre-configuration team.
- www.cert.europa.eu



CERT workshop Oct. 2011

- Topic: Addressing NIS aspects of cybercrime.
- Organized with Europol
- Conclusions
  - Cooperation between CERTs and LEAs is beneficial
  - Trust is key
  - Formal and informal information exchange and collaboration should co-exist
  - Care should be taken about protocols, security clearances, physical security, etc
  - When handling computer incidents, cooperation with other actors, e.g. ISPs, is particularly relevant.
  - When sharing information and cooperating cross-border, legal aspects should be taken into account.

www.enisa.europa.eu

21

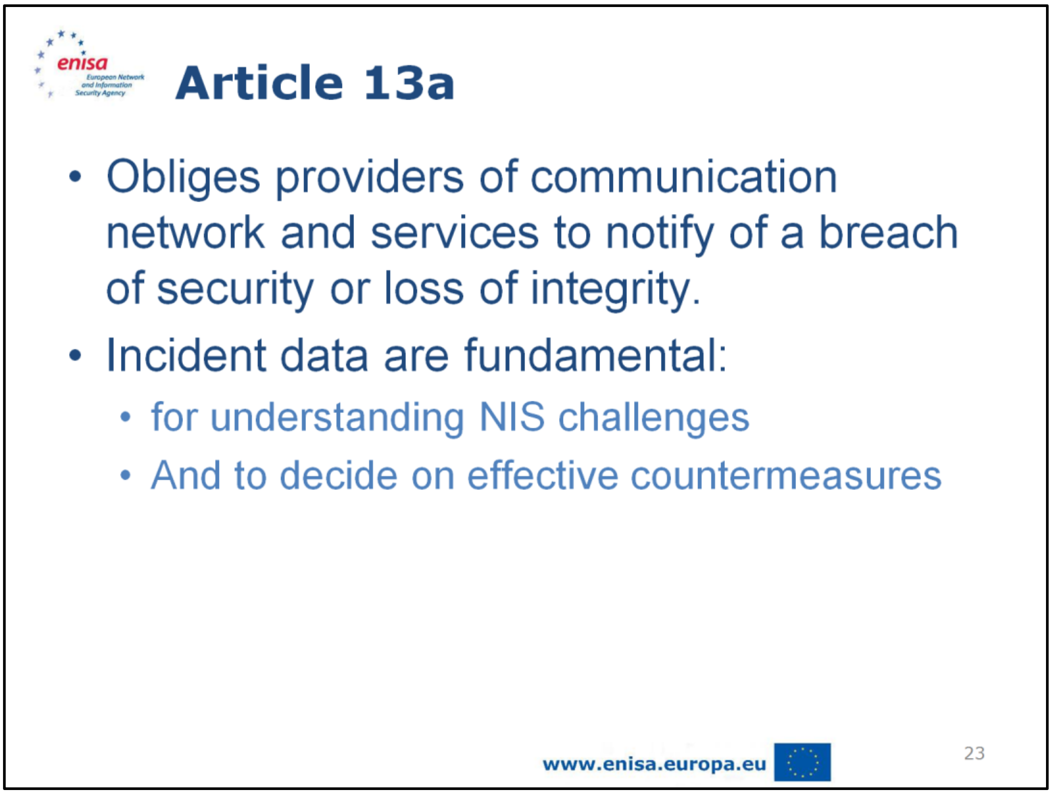
Majority of participants marked this event as an important milestone for both communities in enhancing their cooperation in practice. Most participants welcomed the initiative as this was the first time representatives from both CERT and LEA communities from all over Europe were put together to discuss and debate on the fight against cybercrime and how both communities could improve their collaboration in order to enhance this cooperation practically. The importance of a continuation of these discussions is clear. The ENISA/Europol workshop is a suitable model for future discussions of this kind.

Increased dialogue with Europol to explore possibilities for collaboration and cooperation and overall more efficient coordination.

- Memorandum of Understanding
- Joint workshop for CERTs in Prague (3-4 Oct.)

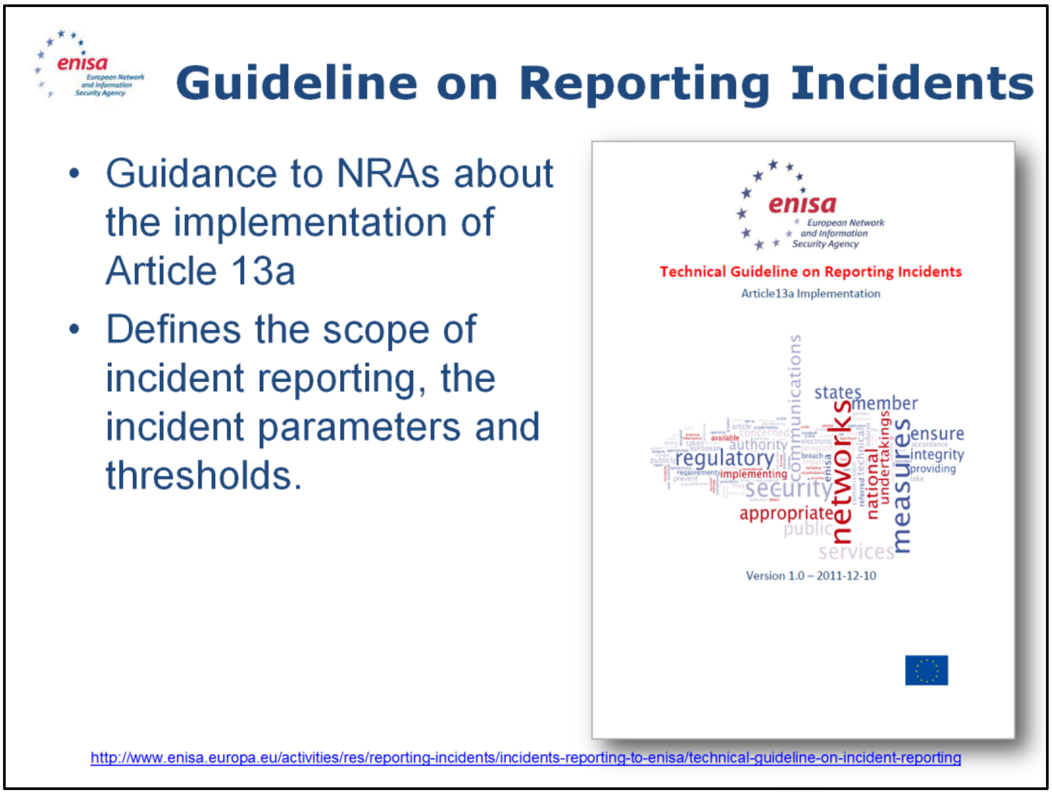
89% of EU MS represented (24 out of 27 EU MS were represented + 3 EEA countries (Iceland, Norway and Switzerland)

ARTICLE 13A



Article 13a

- Obliges providers of communication network and services to notify of a breach of security or loss of integrity.
- Incident data are fundamental:
  - for understanding NIS challenges
  - And to decide on effective countermeasures



Guideline on Reporting Incidents

- Guidance to NRAs about the implementation of Article 13a
- Defines the scope of incident reporting, the incident parameters and thresholds.

Technical Guideline on Reporting Incidents

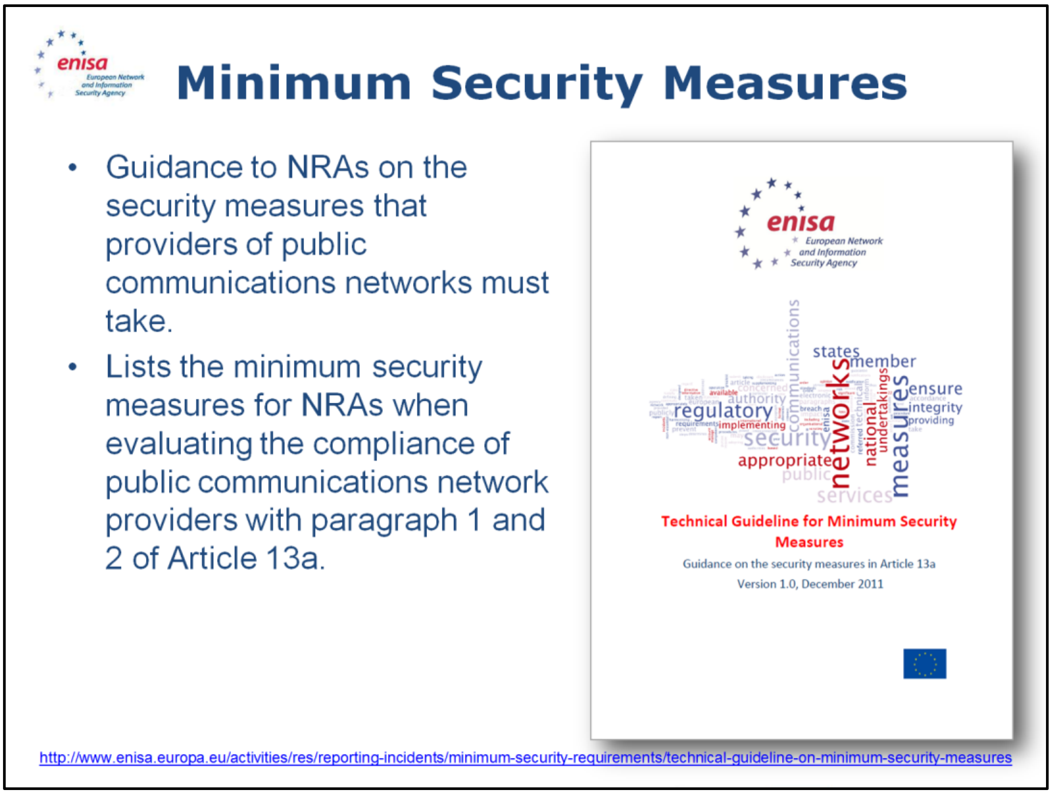
Article13a Implementation

Version 1.0 – 2011-12-10

http://www.enisa.europa.eu/activities/res/reporting-incidents/incidents-reporting-to-enisa/technical-guideline-on-incident-reporting

Guidance to NRAs about the implementation of Article 13a

- The annual summary reporting of significant incidents to ENISA and the EC
- The ad hoc notification of incidents to other NRAs in case of cross-border incidents.



Minimum Security Measures

- Guidance to NRAs on the security measures that providers of public communications networks must take.
- Lists the minimum security measures for NRAs when evaluating the compliance of public communications network providers with paragraph 1 and 2 of Article 13a.

enisa
European Network and Information Security Agency

Technical Guideline for Minimum Security Measures

Guidance on the security measures in Article 13a

Version 1.0, December 2011

http://www.enisa.europa.eu/activities/res/reporting-incidents/minimum-security-requirements/technical-guideline-on-minimum-security-measures

- Gives guidance to NRAs about the security measures that providers of public communications networks must take to ensure security and integrity of these networks.
- Lists the minimum security measures NRAs should take into account when evaluating the compliance of public communications network providers with paragraph 1 and 2 of Article 13a.

Contact

European Network and Information Security Agency

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

http://www.enisa.europa.eu