Identifying Trustworthy Networks, Devices & Software in the EU

Udo Helmbrecht

Executive Director

European Union Agency for Network and Information Security

27th March 2014

Securing Europe’s Information Society

Operational Office in Athens

Seat in Heraklion

ENISA activities

Recommendations

Smart Grid Threat Landscape and Good Practice Guide

Trusted e-ID Infrastructures and services in EU

Good Practice Guide for securely deploying Governmental Clouds

ENISA Threat Landscape 2013

Policy Implementation

Mobilising Communities

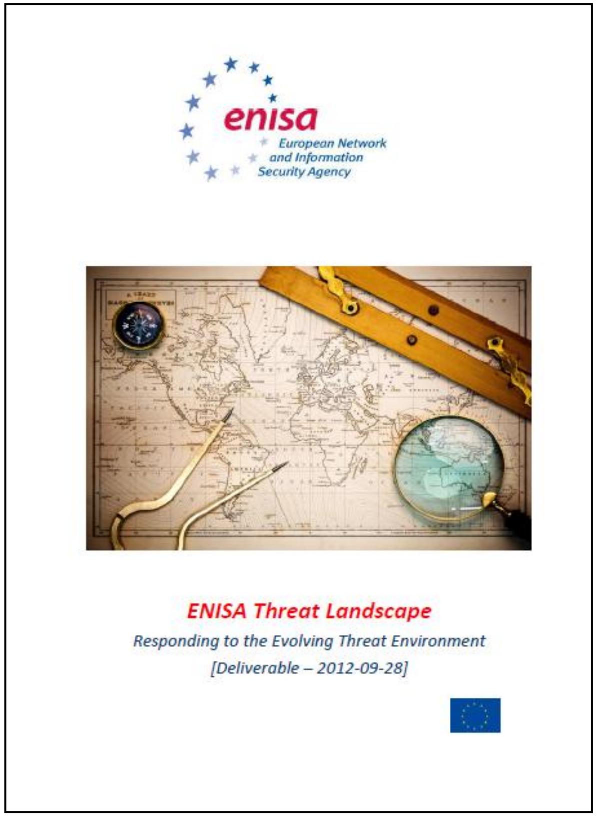
Hands on

enisa European Network and Information Security Agency

CERT Exercises Handbook

Document for teachers

Deliverable – 2012-11-26



enisa

European Network and Information Security Agency

ENISA Threat Landscape

Responding to the Evolving Threat Environment

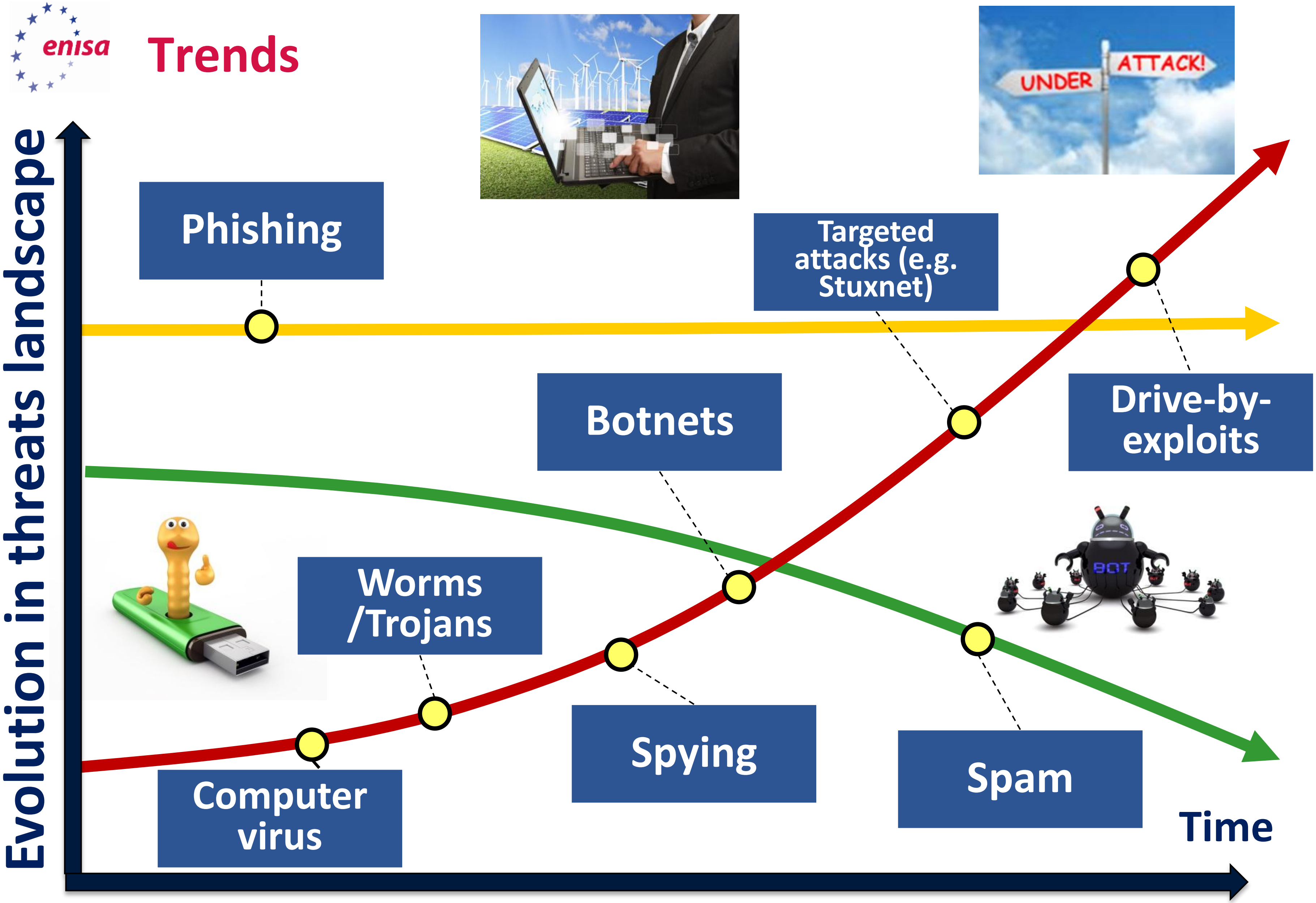
[Deliverable – 2012-09-28]

Security Landscape

Risk = Asset, Threat, Impact

Interesting report links:
http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape

Trends



Phishing

Targeted attacks (e.g. Stuxnet)

Botnets

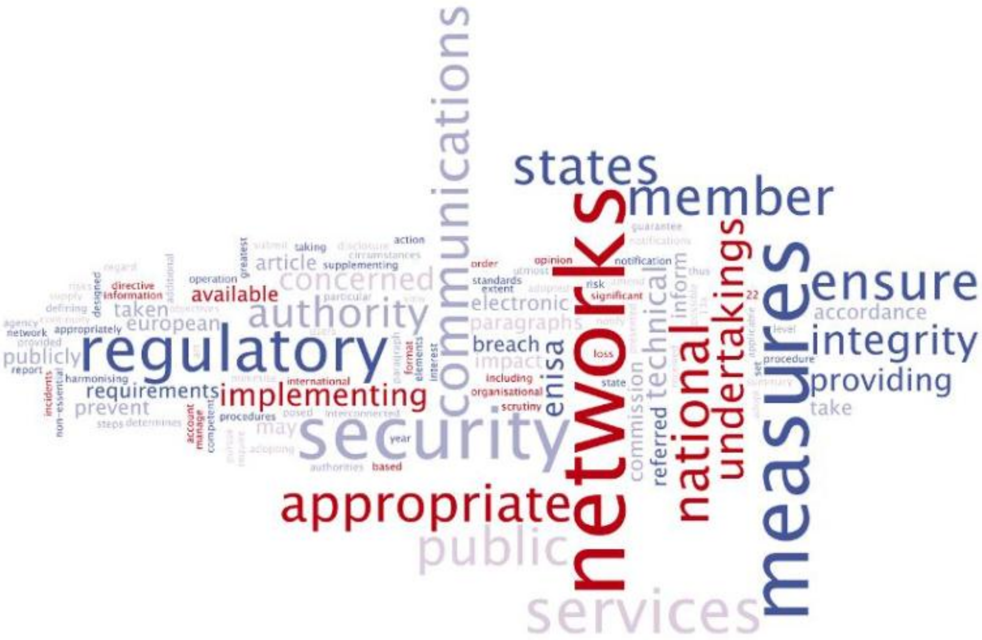
Drive-by-exploits

Worms /Trojans

Computer virus

Spying

Spam



EU Policy Context

EU Policy context (1)

- EU Digital Agenda – COM(2010)245

- EU Cloud Strategy – COM(2012) 529

- EU Cyber Security Strategy – JOIN(2013)1

EU Policy context (2)

- Proposal for a Network & Information Security Directive - COM(2013)48
- Proposal for a reform of the data protection Regulation – COM(2012)11
- Proposal for a Regulation on electronic identification and trust services for electronic transactions in the internal market – COM/2012/0238
- Proposal for an EU Connected Continent Regulation - COM(2013) 627

EU Cyber Security Strategy

- Five strategic objectives defined.

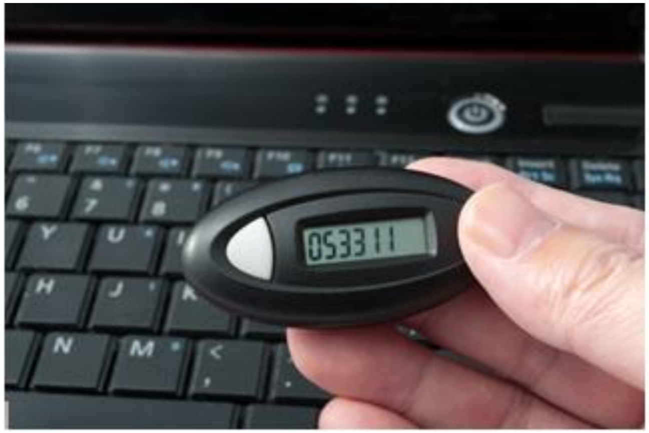
  Objective 4 of the strategy:

  - Developing the industrial and technological resources for cybersecurity

- The Commission asks ENISA to:
  - Develop, in cooperation with relevant stakeholders, technical guidelines and recommendations for the adoption of NIS standards and good practices in the public and private sectors.

ENISA Technical Guidelines

eIDAS: Security requirements for Trust Service Providers

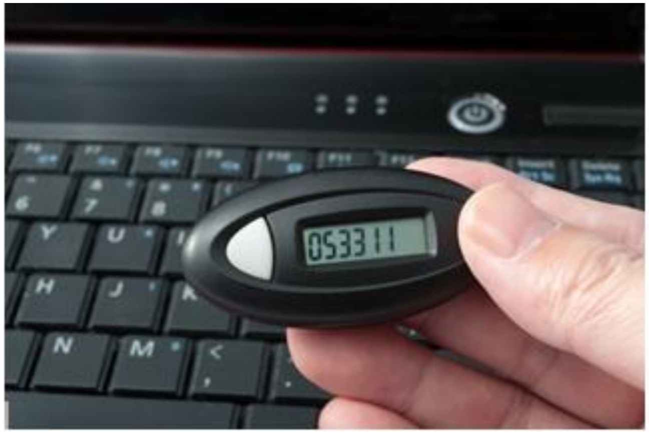


- 2012: Art. 15 of the draft eIDAS regulation (1st stage)
  - Art.13a and Art.4 can serve as functional models for the implementation of Art. 15

- 2013: Minimal security requirements (2nd Stage)

  ENISA produced 3 studies
  - Security framework of trust service providers
    - Organisational aspects of trust service providers operations (regulations, standards, compliance etc.)
  - Risk-assessment at trust service providers
    - Guidelines for trust services providers on how to identify, assess and characterize the existing threats to trust services, how to identify the critical assets and their vulnerabilities and how to determine and minimize the risk

eIDAS: Security requirements for Trust Service Providers

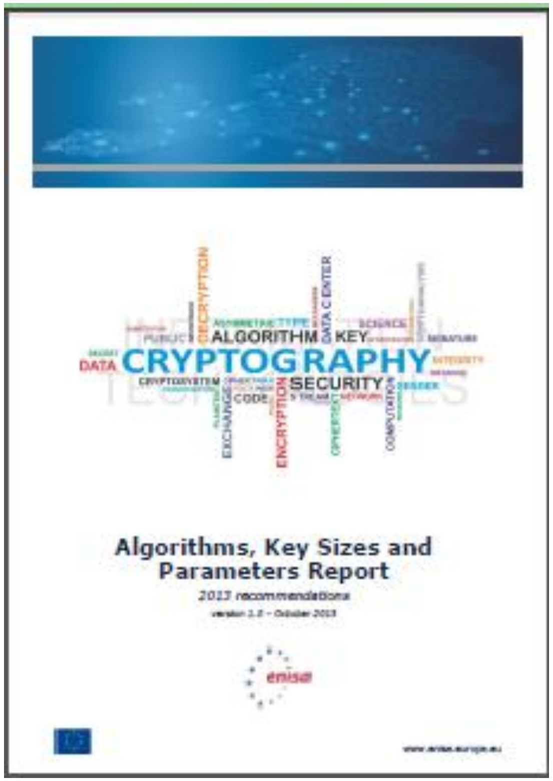


- 2013 (continuation)
  - Mitigating the impact of security incidents in trust service providers
    - Guidelines to trust services providers on how to prevent and minimize the impact of security breaches and losses of integrity on their services

- 2014: Auditing framework for trust services (3rd stage)
  - Technical guidelines for independent auditing bodies and supervisory authorities on the implementation of audit schemes for trust service providers in MS

Algorithms, Key Sizes & Parameters Report

- Work carried out in collaboration with cryptographers from KUL and University of Bristol.
- Technical document addressed to decision makers, specialists designing and implementing cryptographic solutions.
- Collates recommendations for algorithms, keysizes, and parameters
- Addresses the need for a minimum level of requirements for cryptography across the EU.



Algorithms, Key Sizes and Parameters Report

2013 recommendations

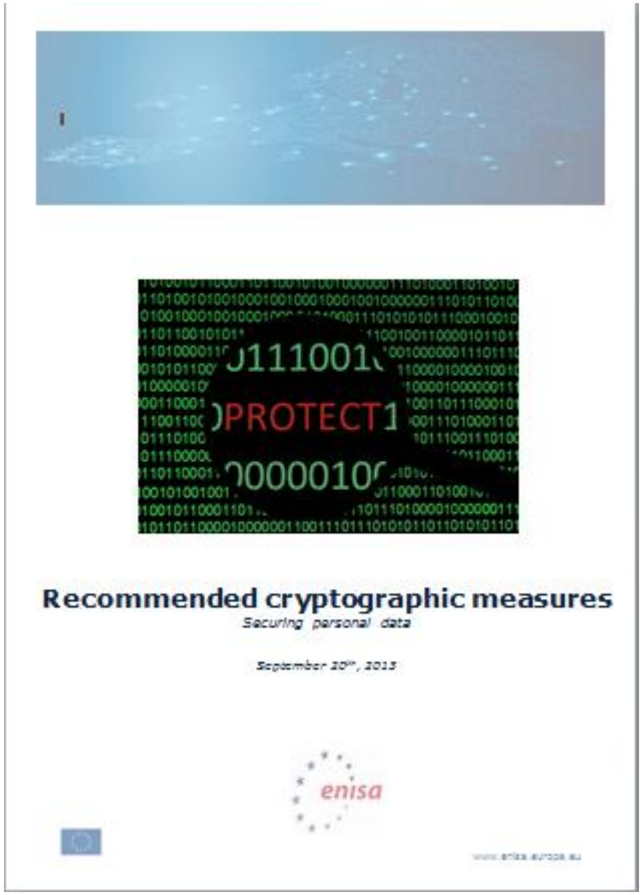
version 1.0 – October 2013

enisa

www.enisa.europa.eu

Securing Personal Data

- Addresses the protection measures applied to safeguard sensitive and/or personal data,
- Shows how information technology users, who have a basic knowledge of information security, can employ cryptographic techniques to protect personal data.
- Addresses the need for a minimum level of requirements for cryptography across European Union (EU) Member States (MSs) in their effort to protect personal and/or sensitive data.



Recommended cryptographic measures

Securing personal data

September 30th, 2013

enisa

www.enisa.europa.eu

Standards and Certification

The Importance of Standards

- Improving efficiency and effectiveness of key processes.
- Facilitating systems integration and interoperability
- Enabling different products or methods to be compared in a meaningful manner.
- Providing a means for users to assess new products or services.
- Structuring the approach to deploying new technologies or business models.
- Simplification of complex environments.
- Promoting economic growth.

The New ENISA Regulation

- The former ENISA regulation identified the following role for ENISA:

  (g) track the development of standards for products and services on network and information security;

- The new regulation is more ambitious:

  (d) support research and development and standardisation, by:

  (i) facilitating the establishment and take-up of European and international standards for risk management and for the security of electronic products, networks and services;

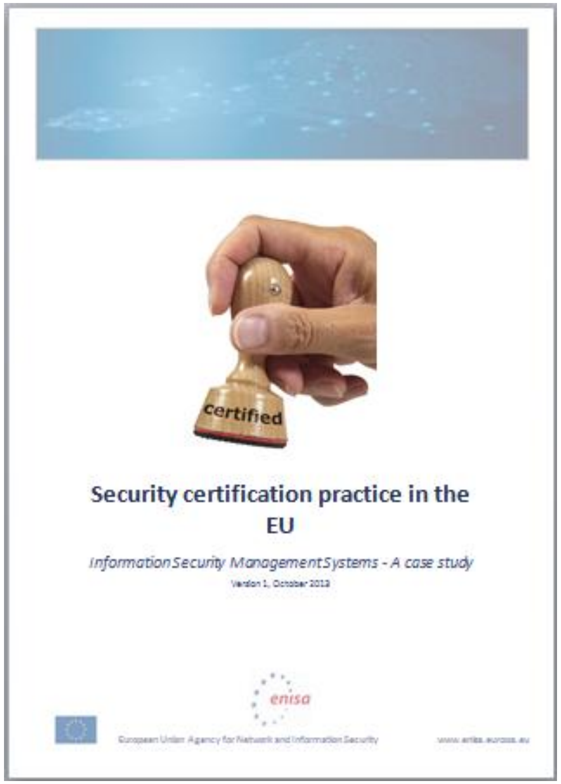
Standards – ENISA Activities

- ENISA regularly looks at the issue of standardisation within ongoing projects.
- In the past we have released specific deliverables related to the standardisation process.
- The Agency has an MoU with ETSI.
- We participate in the Cyber Security Coordination Group.
- ENISA worked with ETSI developing a list of Cloud Standards under the EC Cloud Strategy

Certification

‘When considering introducing certification for privacy/data protection, the European Commission together with national policy makers should link such initiatives with existing national accreditation structures’

‘Companies should not be able to get certificates without really having implemented the processes and controls that have been written down in the audited documents. The national policy makers should ensure enforcement of such requirements for genuine compliance for instance by applying sanctions and/or ad-hoc assessments carried on by third parties’



Security certification practice in the EU

Information Security Management Systems - A case study

Version 1, October 2013

enisa

European Union Agency for Network and Information Security

www.enisa.europa.eu

Cloud Security Certification

- Implementing EC Cloud strategy: Selected Industry Group on Certification Schemes
- Outcomes:
  - ENISA paper: Certification in the EU Cloud Strategy
  - Cloud Certification Schemes List: https://resilience.enisa.europa.eu/cloud-computing-certification
  - Cloud Certification Meta-framework: ENISA is the project leader of this task together with a drafting team of the SIG.

Security in the Cloud and Data Protection

Interesting report links:
http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape

ENISA’s Cloud Security work

- 2009 Cloud computing risk assessment
- 2009 Cloud security Assurance framework
- 2011 Security and resilience of GovClouds
- 2012 Procure secure (Security in SLAs)
- 2013 Critical cloud computing
- 2013 Incident reporting for cloud computing
- 2013 Securely deploying GovClouds
- 2013 Support EU Cloud Strategy - CCSL

- 2014 Cloud Certification Meta-Framework
- 2014 Procurement security in GovClouds
- SecureCloud 2014 Conference (ENISA, CSA, FOKUS)

SecureCloud 2010

- March 16-17, 2010

SECURECLOUD2012

FRANKFURT AM MAIN // 9-10 MAY

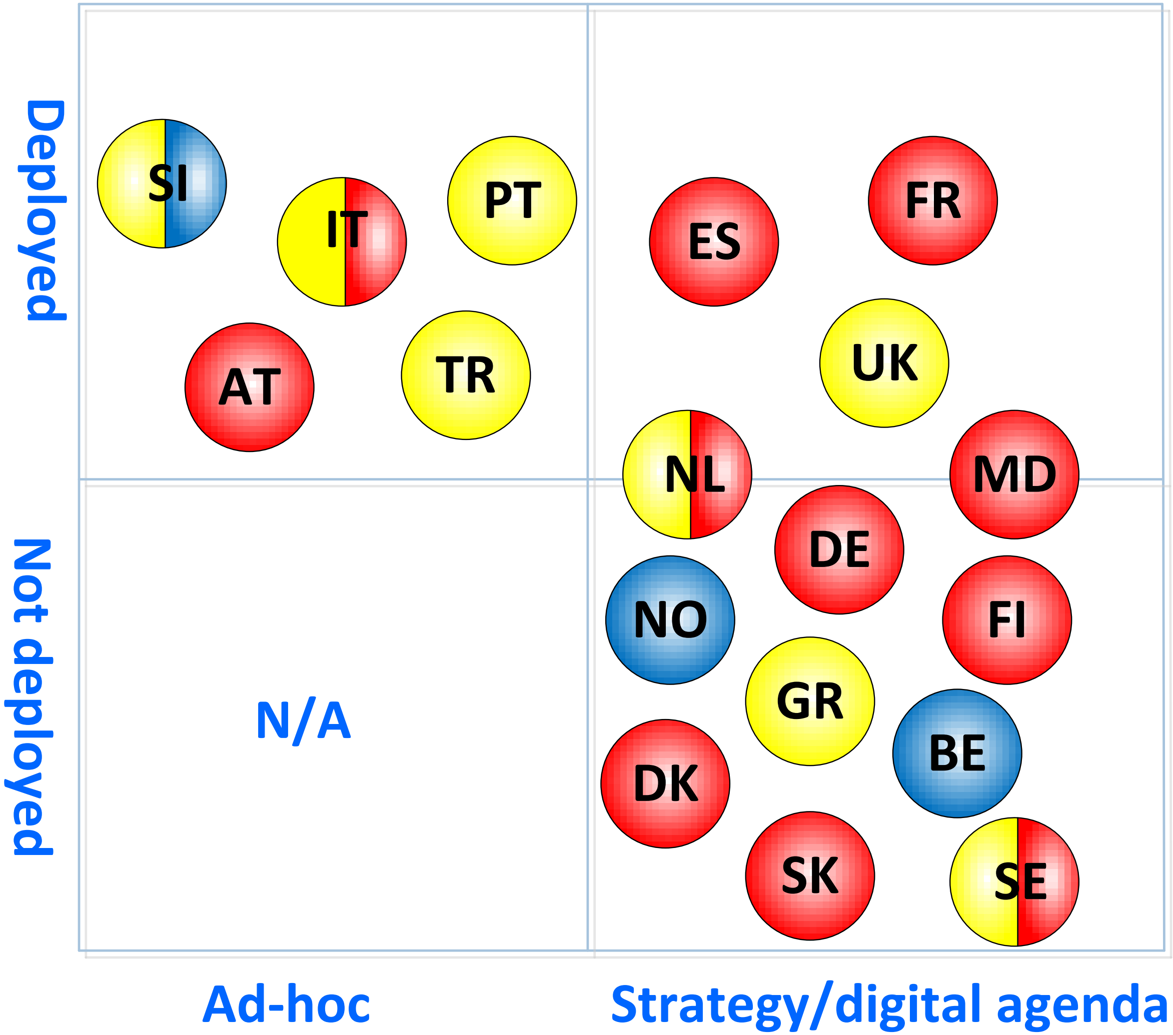
SECURECLOUD2014

1–2 APRIL 2014 // AMSTERDAM

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing

Governmental Clouds in Europe

September 2013



(red = private, yellow = public, blue = community)

Data Protection in the Cloud

- **SME Risk assessment guide update is ongoing**
  - Law enforcement seizures and forensics
  - Foreign jurisdictions
  - Compliance to Data Protection legislation

- **EU citizens, companies, governments concerned with:**
  - Citizens' private data
  - Industry's intellectual property

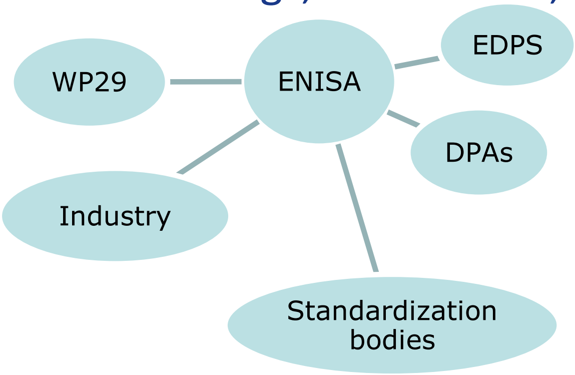
- **Crypto in cloud computing**
  - Crypto can be used to mitigate some of these risks
  - But crypto cannot replace trust in the provider

Privacy and data protection

- **Assist the technical implementation of legal obligations**
  - E.g. data minimization by example, privacy by design & default, data portability & data erasure techniques

- **Support everyday activities of DPAs and data controllers**
  - E.g. minimum security measures, sectorial PIA schemes, self-audit privacy frameworks, certification schemes

- **Analyse privacy needs in new technologies**
  - E.g. Cloud computing, Internet of things, smart cities, big data



Cooperation With The Private Sector

The NIS Platform

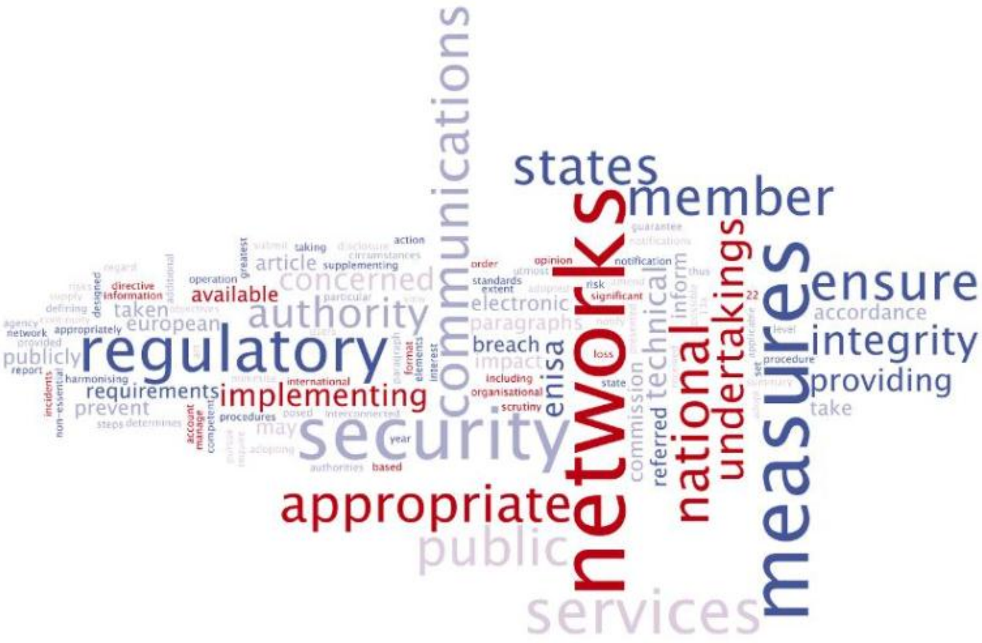
The NIS Platform provides a framework for supporting collaboration between public and private sectors on NIS policy issues – powered by the EC, supported by ENISA

ENISA is supporting this initiative:

- to ensure exchange of expertise on policy and operational aspects
- the provision of good practice guides
- to facilitate collaboration and awareness on NIS issues

3 working groups

- WG1 on risk management, including information assurance, risks metrics and awareness raising;
- WG2 on information exchange and incident coordination, including incident reporting and risks metrics for the purpose of information exchange;
- WG3 on secure ICT research and innovation.



Conclusions

Conclusions

- ENISA works together with operational communities to identify pragmatic solutions to current security issues.

- We issue concrete advice on how to improve system security and which implementations to favour.

- The solutions we propose are based on industry best practice and are therefore known to work.

- By working in this way, we put security to the service of EU industry and improve the competitiveness of our industries.

Questions?

Follow ENISA: f in You Tube