

Security and Resilience of Critical Communications Networks and Services

ENISA's Contribution

Vangelis Ouzounis & Marco Thorbruegge

Senior Experts - Network Security Policies & CERTs Technical Competence Department

ENISA



Context

- ★ ICT vital for the economy & society
- communication networks & services are critical
- constantly changing threat environment
- * security and resilience a major challenge for all





Resilience



ability of a system to provide & maintain an acceptable level of service in face of faults (unintentional, intentional, or naturally caused) affecting normal operation





Threat Environment

- significant physical disasters affecting CIIPs
- complex networks and services
- low quality of software and hardware
- asymmetric threats allowing to attack critical CII from great distances
- increasing organised cybercrime and industrial espionage
- lack of international agreements and regimes,
- lack of well functioning operational mechanism at the international level



1 at the internation...

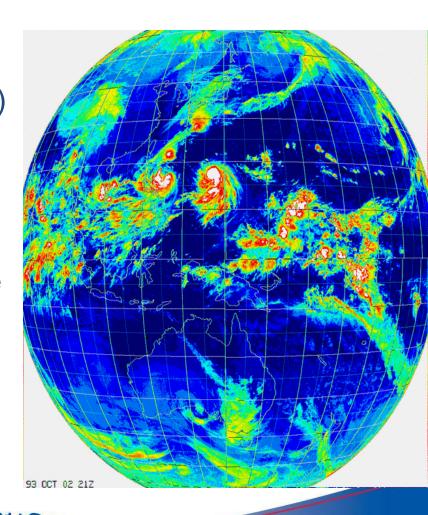
1 at the internation...

1 at the internation... 010010010001011



Threat Levels

- global (e.g. DNS)
- state (e.g. state sponsored attacks)
- societal (e.g. physical phenomena)
- economy (e.g. attacks addressing more than one sector)
- * sector (e.g. attacks against finance sector)
- company/individual (e.g. hostile activities towards a company or individuals)







Our Challenges

- CIIP global issue without global governance
- uneven and uncoordinated national & European activities
- ★ lack of comprehensive national risk management processes
- ★ insufficient co-operation among private and public stakeholders
- lack of efficient Information sharing & good practice guides
- insufficient experience in national and pan European exercises







EU Communication on CIIP

Preparedness and Prevention

- Strategic pan European Public Private Partnership for Resilience (EP3R)
- European Forum for information sharing between Member States
- Baseline Capabilities of National/Gov CERTs
- Cross-country co-operation between National/Gov CERTs

Detection and Response

★ European Information Sharing and Alert System (EISAS)

Mitigation and Recovery

- National Contingency Plans and Exercises
- Pan-European exercises on large-scale network security incidents
- Reinforced cooperation between National / Governmental CERTs

★ International cooperation

European and global priorities, principles and guidelines on long term Internet resilience and stability





ENISA's Resilience

Collectively evaluate and improve resilience of European public eCommunications Networks

Stock taking

- Policies/Strategy
- Operators Measures
- Technology

Gap Analysis

- Gap Mitigation
- Good practices
- Guidelines

COM

- Recommendations
- Good practices
- PPP and Forum
- Exercises
- New Stock Takings

2008 2009 2010

By 2010, the Commission and at least 50% of the Member States have made use of ENISA recommendations in their policy making process



Stock Takings & Analysis



25 countries

- 23 MS
- 2 EFTA countries

Policy

http://www.enisa.europa.eu/doc/pdf/resilience/stock_taking_final_report_2008.pdf

Provider Measures

http://www.enisa.europa.eu/doc/pdf/deliverables/enis a_network_provider_measures_on_resilience.pdf





Policies & Strategy – 10 Recommendations authyagency

- co-ordination mechanisms to enhance consistency and coherence of national strategies and policies
- ★ soft-law instruments (e.g. guidelines, recommendations, good practices)
- ★ enforcement practices =? operators' compliance
- ★ implement a holistic and integrated national risk management process
- ★ assess the degree of operators' adherence to preparedness measures
- ★ one State = 1 national/Gov CSIRT/CERT
- ★ need for more good practice guidance ENISA's chance!
- establish national trusted information sharing schemes
- ★ cost effective incident reporting procedures based on good practices
- ⋆ need for a consistent pan European policy and strategy





Information Sharing Exchanges

- assess impact of incidents (security breaches, network failures, service interruptions)
- identify, analyse, and adopt sector wide preparedness measures
- continuously review the implementation of adopted measures
- Provide unique, strategic insights to policy and decision makers



http://test.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange





Upcoming Good Practice Guides

Incident Reporting

★ good practice guide on how to implement article 13 of new Telecom Package

National Exercises

good practice guide for designing/implementing national & first pan European exercise

Providers Measures

guidelines on cooperation, mutual aid practices, business continuity exercises, third party dependencies

DNSSec Deployment

DNSSec deployment good practices guide, cost benefit analysis, Trusted Anchor Repositories policy and good practices

Cloud Computing

- ★ Resilience features of cloud computing
- **Priorities of Research On Current and Emerging Network Trends**
 - research trends, R&D areas and priorities for EU funded R&D Programmes
- Standardization activities in resilience
 - Identification of standards and gaps





ENISA's Impact on CERTs/CSIRTs

National / Government CSIRTs in National / Government CSIRTs in Europe 2005 **Europe spring 2009** •PLANNED: •PI US: Finland Austria •Belgium France Czech Belgium Germany Republic Bulgaria Hungary Cyprus Estonia The Iceland Italy Netherlands •Latvia Ireland Norway Greece Lithuania Sweden Luxembourg Spain •UK Poland Portugal Slovakia •Outside EU: Most former

- Soviet Republics
- South Africa







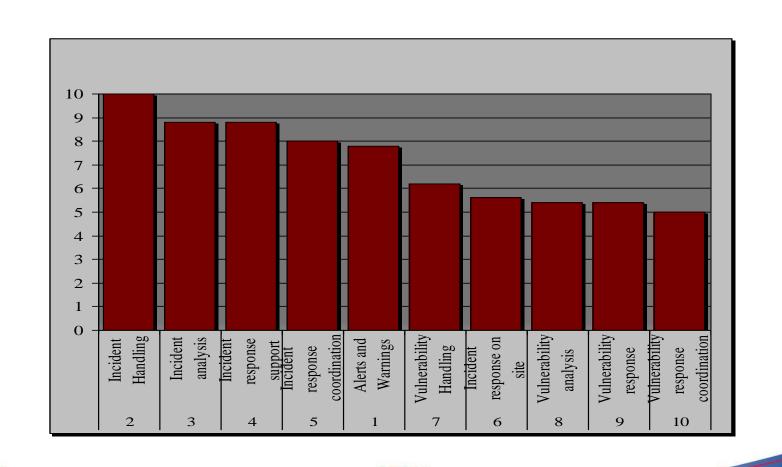
CERTs Activities

- ✓ Continue facilitation of the setting up of CERTs/CSIRTs and stay in close relation to the various CERT/CSIRT communities
- ✓ CERT Exercises: the next step to achieve impact
- ✓ Prepare CERT good practice collection: the role of national CERTs/CSIRTs (D4)





Typical CERT Profile









WP 2010 - Resilience

- Contribute to EU's CIIP action plan
- Promote Findings & Recommendations
- First pan European Information Sharing Exchange
- Help Member States adopting good practices
- Policy Recommendations for Response & **Recovery Measures**
- Take Stock of new Areas, New Good Practices
 - **Botnets**
 - resilience metrics
 - socio-economic barriers to information sharing
 - interconnection and BGP
 - end-end security architectures
 - national risk management processes





WP 2010 - CERTs

- ➤ Good practice in providing CERT services based on the survey from 2009
- Facilitate cooperation and information sharing
- pan-European cooperation among national CERTs
- ➤ 5th ENISA Workshop (CERTs in Europe)
- •- the role of national CERTs in national and international exercises
- ➤ Continue facilitation of the setting up of CERTs
- continue to develop tools for strengthening the CERT community







Conclusions

 security and resilience of Critical Networks and Services extremely important

uneven and uncoordinated national &
 European activities leave open security holes

★ Com's Communication in CIIP a milestone; paves the way for a holistic pan European strategy

- strategic Public & Private Partnership is needed to enhance co-operation
- ★ ENISA's role stronger than ever to meet the challenges

