

Resilience of Public eComs Networks

Strategy, Policies, Providers Measures

Dr. Evangelos OUZOUNIS

Senior Expert – Security Policies

Technical Department

ENISA

evangelos<dot>ouzounis<at>enisa<dot>europa<dot>eu

Stock Takings & Analysis



25 countries

- 23 MS
- 2 EFTA countries

Policy Stock Taking - http://www.enisa.europa.eu/doc/pdf/resilience/stock_taking_final_report_2008.pdf

Providers Measures Stock Taking

http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_network_provider_measures_on_resilience.pdf



Polices & Regulations - Findings

- ★ different approaches and maturity in MS' policy, regulatory measures, & operational capabilities
- ★ huge complexity and lack of co-ordination mechanisms (e.g. 5-8 authorities);
- ★ PPPs, an interesting and widely used model in key MS, e.g.
- ★ no reporting duties, no auditing
- ★ interest in exercises but ... a few do it so far!
- ★ national risk management ... not widely deployed
- ★ pan European activities fragmented, overlaps among players,

Policies & Regulations - Recommendations

- ★ 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 governmental CSIRT
- ★ 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
- ★ act local but ... think and co-operate global!

Policy & Regulations - 2009 Activities

★ Information Sharing

- ★ stock taking and desktop research
- ★ Joint ENISA-ARECI workshop on Good Practice on Information Sharing, Lisbon, 18-19 May

★ Incident Reporting

- ★ only related to resilience and security (privacy is out of context)
- ★ help national bodies (e.g. NRA's) to understand the complexity of incident reporting (e.g. Article 13 of new Telecom Package)
- ★ topics include: serious incidents, when are reported, to whom, how, when, response and recovery measures, ex-post assessment, media relations,

★ National Exercises

- ★ how to set up and/or run exercises at regional or national level
- ★ Topics include: categories and format, techniques assessing preparedness measures, organisation and management issues, involvement of regional/national public authorities, ex-post exercises assessment, cost of conducting different types of exercises

Providers - Findings

- ★ Network resiliency is a high priority – Top Mgmt support
- ★ Average of 99.9% availability: 10 hours downtime a year
- ★ High process maturity – achieved or sought
- ★ Full range of measures deployed
 - ★ Technical measures
 - ★ Network Management processes
 - ★ Risk Management
 - ★ Business Continuity Management
- ★ Due to the variation in types of operators blanket policies are unlikely to be effective
- ★ Operators appear to go alone but seek support from external partners

Providers - Recommendations

- ★ co-operation among providers (and/or public authorities) on threats and vulnerabilities management
- ★ co-operation among providers (and/or public authorities) on dependencies
- ★ co-operation among providers on mutual aid procedures during crisis
- ★ analyse gaps and identify mitigation measures and strategies
- ★ aim for defined processes in Network Mgmt, RM, BCM
- ★ develop key measurements, agree on success targets and good practices
- ★ follow a soft-law approach, give emphasis on guidelines and recommendations
- ★ participate in national (or pan European) Information Schemes
- ★ co-operate with national/governmental CERTs

Providers - 2009 Activities

- ★ Gap Mitigation Guidelines (December 2009)
 - ★ cooperation and mutual aid practices
 - ★ sustaining resilience throughout network evolution
 - ★ business continuity exercising
 - ★ coping with third party dependencies (e.g. modelling dependencies, shared responsibility, cross-border dependencies)
- ★ Gap Analysis through Virtual Group of experts
 - ★ identify and assess good practice measures for communication networks
 - ★ May to September 2009, one physical meeting end of April
 - ★ four virtual meetings via phone + internet
 - ★ PSG members are welcome!
- ★ Feedback from stakeholders
 - ★ September 2009 thematic workshop (discussion on draft guidelines)
 - ★ Request for comments from stakeholders

WP 2010 and Beyond - Ideas

- ★ Contribute to EU's strategic pan European PPP on security and resilience of critical information infrastructures
 - ★ promote ENISA's recommendations and good practices guides to public and private authorities
 - ★ underpin Member States' and Providers efforts to adopt them
 - ★ help Member States to run the first pan European Exercise by 2010
- ★ Take Stock, Analyse and Develop Good Practices and/or Recommendations
 - ★ identifying, measuring, disinfecting and defending against Botnets
 - ★ resilience metrics
 - ★ socio-economic barriers to public private co-operation
 - ★ interconnection issues
 - ★ response and recovery measures – policy recommendations
 - ★ end-end security architectures including resilience and security of middleware and service provisioning platforms
 - ★ national risk management processes

EU Communication on CIIP

★ Preparedness and Prevention

- ★ Baseline Capabilities of National CERTs
- ★ Strategic pan European Public Private Partnership for Resilience (EP3R)
- ★ European Forum for information sharing between Member States

★ 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