

Improving Resilience in Public eCommunication Networks

P. Saragiotis

.SE DNSSEC and IPv6 Workshop



Activities for 2008 and beyond

- ★ Multi-annual Thematic Programmes
 - **★** Strategic priorities for ENISA
 - ★ Implemented through a number of Work Packages
- Current focus on:
 - ★ Improving Resilience in European e-Communication **Networks**
 - ★ Developing and Maintaining co-operation between **Member States**
 - ★ Identifying Emerging Risks for creating trust and confidence
 - Building information comments
 Enterprises (Preparatory action)

 CONTROL OF THE PROPERTY OF THE ★ Building information confidence with Micro





Resilience



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





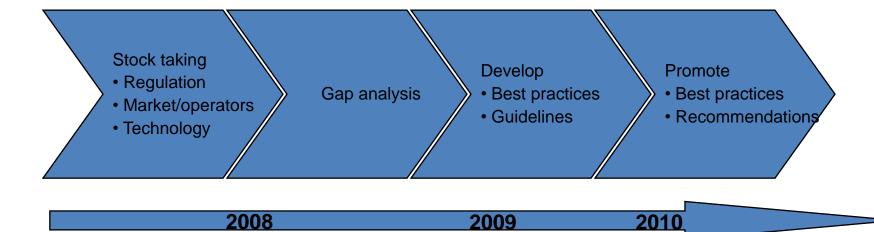
Network resources resilience

- ★ The main aim of resilience is for faults to be invisible to users.
- ★ Real-Time Applications Demand that Resilient end-to-end Network Services Be Extended Consistently Across the Network.
- ★ The classification of a networks resilience has to be given from the availability and performance perspective.



Improving Resilience in European e-Communication networks

Collectively evaluate and improve resilience in European e-Communication networks



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





WPK 1.3 – Background Info

⋆ Objectives

★ Analyze current and emerging technologies used by network and service providers to enhance the resilience of their operations

★ Scope

★ IP backbone technologies

★ Stakeholders

- ★ Equipment vendors, network operators, services providers
- * Research institutes and standardization bodies
- ★ Policy makers

★ Target Group

- ★ Regulators and Policy Makers
- ★ Operators
- ★ Vendors





Approach - Status

- Selection of topics & stakeholders
 - ★ Consultation workshop, Q1 08, Brussels
- ★ Consultation with stakeholders
 - ★ Prepared a Questionnaire, Q3 08
 - **★** Conduct Interviews, Q3 & Q4 08
- * Analysis of resilience enhancement of existing and emerging technologies
 - ★ Compile a report for the "Resilience Features", Q4 08
 - ★ Present the findings of the Interviews in Workshop 12th and 13th November, Brussels
 - ★ Conduct analysis of interview findings, Q4 08
- Validation of findings with experts and stakeholders
 - **★** Q4 08 to Q1 09









Technologies that may improve Resilience

★ IPv6

★ A technology replacing IPv4, the internet protocol.

★ DNSSEC

★ Security extensions improving the security of Domain Resolution System.

★ MPLS

* A protocol used by operators in IP backbones, replacing Frame Relay and ATM.





Existing Consultations and Reports

- ★ Hurdles and Triggers for the Deployment of IPv6 Technology, public consultation by INFSO
 - ★ Identified triggers, hurdles and worthy initiatives
 - ★ The average timeframe for wide deployment is 4 to 5 years
- ★ IPv6 among CENTR members, a survey by .SE
 - ★ If there is demand
- ★ World Wide DNSSEC Deployment

10100100100010

- ★ http://www.xelerance.com/dnssec/
- **★** DNSSEC statistics
 - * https://www.iks-jena.de/leistungen/dnssec.php





Stocktaking Targets

★ Interview a small number of Network **Operators and Service Providers**

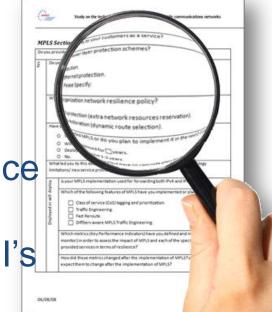
Classify the reasons for implementing / not

★ Investigate if the technologies enhance / are expected to enhance resilience

★ Quantify this enhancement to KPI's

Spot customers reactions

★ Identify success and/or failure stories







Possible Recommendations

- ★ Opinion on consultation for implementing **DNSSEC on DNS root**
- ★ Best practices for providing recursive resolution service with DNSSEC validation
- * Best practices for the implementation of the three technologies for SME's
- ★ Incentives for the implementation of IPv6, DNSSEC
- * Require IT procurements to include IPv6 capable products and systems







An in-depth look on the ENISA activities on resilience...



•Workshop on "Improving Resilience in European e-Communication Networks", Brussels,12-13 November 2008

- ★ Two days workshop, where:
 - ★ the findings of the stock taking activities carried out during 2008 will be presented;
 - ★ including the possible directions in terms of recommendations that the Agency will follow in the course of next year;
- ★ For further information:
 - •http://www.enisa.europa.eu/sta/workshop2008





Summarizing

- ★ Importance of the Resilience of public eCommunication networks
- ★ ENISA is working with all sector actors
 - ★ Key target audience are Policy Makers, NRAs and Operators
- ★ Technologies benefits are well recognized however the economical / political incentives have to be made





Thank You

Panagiotis SARAGIOTIS, European Network and Information Security Agency SN Expert - Security Tools and Architectures

Email: Panagiotis.Saragiotis@enisa.europa.eu

★References

- ★http://www.enisa.europa.eu/sta
- ★http://www.enisa.europa.eu/sta/workshop2008

Disclaimer: "The views expressed in this presentation are those of the authors and do not necessarily represent the views of the Agency".

