ENISA's WORKSHOP

Improving Resilience of Public Communication Networks and Services

7th of March 2008, Sofitel Brussels Europe
Place Jourdan 1, 1040 Brussels, Belgium

Preliminary Agenda

Contact:
Dr. Vangelis OUZOUNIS
Senior Expert - ENISA - email: resilience@enisa.europa.eu

1   Context

Reliable communications networks and services are now critical to public welfare and economic stability. Recent attacks on Internet resources and services in Member States revealed the increased vulnerabilities of our Information Society. The experience has revealed that any country or service provider, acting independently, may face difficulties in effectively preventing and responding to this type of attacks which often originate from beyond national and European borders.

Recent Commission Communications[1] highlighted the importance of network and information security for the creation of a single European information space and stressed the importance of dialogue, partnership and empowerment of all stakeholders. The proposed update of the existing Regulatory Framework includes certain measures for the improvement of the security and resilience of public e-Communication Networks.

The European Network and Information Security Agency (ENISA), fully recognising this problem, devised a Multi-annual Thematic Program (MTP) on the security and resilience of public e-Communication networks and services in Europe[2]. The ultimate objective is to collectively evaluate and improve the security and resilience of these networks and services in Europe.

The Agency will reach this goal by analysing how national authorities implement current regulatory measures, assessing how network and service providers of public Communication Networks ensure availability and integrity of their networks and services, and by evaluating whether existing technologies satisfy the needs and requirements of these providers. The stock taking will help the Agency to identify gaps, inconsistencies, but also best practices.

In 2009 the results of the analysis will be compared against trends, recommendations and guidelines proposed by other national, European and global initiatives. Based on an extensive consultation with relevant stakeholders the Agency will then propose guidelines that might contribute to the development of a common regulatory framework for electronic communications in Europe.

2   Scope and format of the Workshop

With this first consultation workshop ENISA is trying to bring together all relevant stakeholders to debate about European policy on preventive, detection, emergency and recovery measures and technologies related to resilience of electronic communications. The result of this workshop will help the agency to scope down its efforts and prioritise on the topics that mostly affect resilience of public communication networks.

---

[1] "i2010 – A European Information Society for growth and employment[1]" & "A strategy for a Secure Information Society",

[2] http://www.enisa.europa.eu/doc/pdf/management_board/decisions/enisa_wp_2008.pdf

The workshop will debate, among others, about business continuity plans, pre-arranged priority restoration, testing of multi-domain networks, critical communications paths and priority communications, protection measures on DNS, traffic and exchange routing, security in BGP, detection of attacks.

The workshop is organised around two thematic areas each corresponding to a breakout session. The themes are 1) regulatory measures, 2) operational security measures deployed by providers and technologies and standards. Each breakout session is organised as open, brainstorming session where participants debate about the topics and the approach that ENISA should take to perform the stock taking exercise. The outcome of each session will be presented in plenary to all participants with the objective to develop a consolidated approach.

3 Profile of Participants

The workshop is open to experts representing stakeholders from national regulatory authorities, national authorities responsible for the definition and implementation of security measures, legal experts on security regulations, providers of public electronic communication networks and services, associations of providers, professional IT security companies, software and hardware vendors of network equipments, research organisations/ universities and standardisation bodies.

4 Agenda

7th of March, Sofitel Brussels Europe	
09:00 – 09:30	Registration and Coffee
09:30 – 09:50	Welcome – Scope of the Workshop *Alain Esterle & Vangelis Ouzounis* *Technical Department, ENISA*
09:50 – 10:10	Policy Context – European Commission's Views and Priorities *Andrea Servida* *European Commission, DG- INFSO-A3*
10:10 – 10:30	Resilient eCommunication Networks *Magnus Nyström* *RSA & member of ENISA's Permanent Stakeholder's Group*
10:30 – 11:00	Coffee Break
11:00 – 11:20	Regulatory measures - lessons learned *Anders Johanson* *Swedish Post and Telecom Agency, chair of IRG WG on Security*
11:20 – 11:40	Provider Measures *Jean-Pierre Coustel* *France Telecom*
11:40 – 12:00	Resilient Technologies and Standards TBD
12:00 – 13:00	Lunch break
13:00 – 15:00	*Breakout Session 1* Regulatory Measures *Moderated by ENISA* *Rapporteur:TBD*	*Breakout Session 2* Operational Measures, Technologies & Standards *Moderated by ENISA* *Rapporteur: TBD*
15:00 – 15:30	Coffee break
15:30 – 16:45	Wrap up of Breakout Sessions – Panel (TBD) *representatives from EuroISPA, EICTA, ETNO, RIPE,CENTR, ….*
16:45 – 17:00	Workshop Conclusions *Alain Esterle* *Technical Department, ENISA*

5