Cybersecurity and Critical Infrastructure in the Energy Community

4th Meeting of the Security of Supply Coordination Group - Subgroup for Electricity

Security challenges in the energy sector

- Moving towards **interconnected**, **digitalized** and **decentralized** systems
- Proliferation of **highly interactive** but **poorly secured** (“user friendly”) information and communication technologies
- **Outsourcing** and **renting** of infrastructures and services
- Increased interdependency and exchange of data among **market players**
- **Protection concepts** and **design rules** of energy facilities not adequate to modern threats
- Dependence on **foreign security technologies** (intregrity and compatibility of components)
- **Cross-border** interconnected energy network – the *“weakest link” and “cascade” effects*
- **Constraints** imposed by security measures – in contrast to real-time-availability requirements
- Availability of **human resources** and their competences, adequacy of procedures
- Evolving **cybercrime** business models, growing powers / interests of cybercrime communities
- Blurring lines between state and non-state actors, **privatization**

Cybersecurity and the Energy Community

- Cyber attacks (Ukraine)
  - **December 2015** – three Oblenergo (DSO) systems compromised for 6 hours (30 SS / 230.000 citizens) - imposed vast damage on systems and data
  - **December 2016** – **Kiyv North** (330 kV SS - SCADA system compromised) causing blackout for 1/5 of Kiyv for one hour – advanced, automated and adaptable malware, simultaneous threat to multiple systems

- NIS Directive (EU) 2016/1148 implementation – PHLG March 2018 Conclusions:
  - Acknowledgement of the necessity to build cybersecurity capabilities and risk management and incident reporting culture in the Energy Community
  - Recommendation to eliminate regulatory gaps and develop cooperation structures, certification framework and research and education programs
  - ECS tasked to explore the incorporation of NIS Directive, take steps and discussions for identification of suitable provisions, and prepare a proposal with adaptations and appropriate timing

NIS Directive

- Build sufficient capacities at national level
  - Adopt a national NIS strategy
  - Designate national competent authorities, single contact points and Computer Security Incident Response Teams (CSIRTs)
- Identify critical infrastructure, operators of essential services (**OES**), and relevant digital service providers
- Build structures for **cross-border** cooperation and exchange of information
  - At strategic level - creating a Cooperation Group of national authorities
  - At operational level - creating a network of national CSIRTs

NIS Directive

- Cumulative conditions for identification of OES
  - provision of a service essential for critical societal / economic activities
  - provision of that service depends on network and information systems
  - an incident would have significant disruptive effects on the provision of that service
- Security and Notification Requirements imposed on OES
  - take technical and organizational measures
    - to secure networks and systems
    - to prevent and manage risks
    - to handle incidents and minimize their effects
  - notify incidents
- Monitoring and enforcement powers

Critical Infrastructure Directive

- Critical Infrastructure
  - An asset, system or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people and the disruption or destruction of which would have significant impact in a MS (CP) as a result of the failure to maintain those functions
  - **European Critical Infrastructure (ECI)** – significant impact on at least two MSs (CPs)
  - ECI sectors: Energy (Electricity, Gas and Oil), and Transport
- Identification of ECI
  - **Criteria** - Sectoral, cross-cutting and trans-boundary, corresponding **Thresholds** (severity of impact),
- Designation of ECI (bilateral / multilateral)
  - Potential / suspected ECI, level of impact, **discussions**, reporting (EC), informing the operator, discretion principles
- Operator Security Plan
  - **Identification** of assets / threat scenarios – **risk** analysis / vulnerability and potential impact / security **measures**
  - Periodic **review**, supervision, Community measures and compliance with agreed **criteria**
- Security Liaison Officers – communication mechanisms
- Threat assessment and reporting (EC), common methodologies, classified information

Cybersecurity and the Energy Community

- Recommendations (based on NIS Directive):
  - Create a Cooperation Group / task force (including CPs and MSs) appoint Liaison officers (focal points)
  - Put in place common certification conditions across the Energy Community
  - Eliminate regulatory gaps
  - Initiate cooperation on the establishment of research and education programmes
  - Develop a common crisis management and rapid emergence response mechanism - Computer Security Incident Response Team (**CSIRT**)
  - Step-up public-private cooperation in cybersecurity

Cybersecurity and the Energy Community

Task Force - consisting of representatives from:

- competent authorities / single point of contacts of CPs
- ENTSO-E
- the CSIRT network
- TSO / security liaison officers (as applicable)
- the Secretariat
- the European Commission
- the ENISA (if possible)
- Observer and Participant countries
- relevant stakeholders (electricity)
- relevant IT environment (services)

ToR / work program / deliverables / a yearly report

Meetings

- twice a year or more, upon a motion of the Chairperson, the Chairperson of SoS CG, the Secretariat
- take part in meetings and activities of the SoS CG

Tasks

- **exchange information and best practice**, discuss modalities, on risks and incidents; on identification of operators and critical infrastructures, on awareness-raising, education programmes and training; research and development
- **discuss capabilities and preparedness of the CPs**, evaluate national strategies, assist CPs in building capacity
- **provide strategic guidance** for the CSIRTs the CSIRTs network
- **engage in discussions** with CPs and MSs on whose territory a potential critical infrastructure is located, and other affected CPs and MSs
- **support** operators of critical infrastructures with best practices, methodological guidelines
- **encourage the use of European or internationally accepted standards and specifications**; discuss them with relevant stakeholders and with relevant organizations

- Study on Cybersecurity in the Energy Community (**electricity** and **gas**)
  - Objective – **building the energy-specific cybersecurity capabilities**, in particular
    - Identify weaknesses, risks and exposure to cyber threats in the energy systems
    - Identify the existing regulatory framework and regulatory gaps for cybersecurity governance
    - Identify the relevant provisions of NIS Directive and provide impact assessment of their implementation
    - Propose the necessary measures for cybersecurity on local level
    - Propose a model for regional cooperation in managing cybersecurity risks and reporting incidents
  - Task 1 – stocktaking review:
    - Make assessment of the level of compliance with the NIS Directive and related acquis and applied EU policies, data protection and confidentiality rules, EU cybercrime conventions and OSCE Confidence Building Measures
    - Identify the institutional framework, competent authorities, international cooperation mechanisms and applicable legal and policy framework relevant for cybersecurity in the domain of energy
    - Identify the standard technologies and practices, existing training, international cooperation, cybersecurity standards, technologies and certification schemes, enforcement authorities
    - Identify potential cyber threats, critical infrastructure and operators exposed, responsible policy authorities, institutional framework and service providers in cybersecurity – both in the energy and in related IT environment

- Study on Cybersecurity in the Energy Community (**electricity** and **gas**)
  - Task 2 – analysis:
    - Based on the analysis of Task 1, identify the legal and regulatory gaps, inconsistencies and potential obstacles for implementation of the relevant provisions of the acquis (NIS Directive)
    - Provide gap analysis compared to standard applied in the EU and ICT products and services in the energy sector, including products and services used by customers (smart grids)
  - Task 3 – proposals (including timeframe):
    - amendments, policies, measures, procedures and recommendations to bridge the identified legal and regulatory gaps and implement minimum framework for cybersecurity of critical energy infrastructure based on the EU legislation (including NIS Directive and Critical Infrastructure Directive)
    - a cooperation mechanism and recommendations for regional cooperation on cybersecurity addressing:
      - Identification of large-scale incidents and crisis that require coordinated response;
      - Establish objectives and modalities for cooperation and propose a blueprint for common mechanisms for cyber crisis management
      - Identify the relevant actors for crisis management and exchange of information
    - harmonization of the certification schemes and common framework for certification, exchange of information, education and training
    - overall impact assessment of the implementation