Study on Cybersecurity

in the energy sector of the Energy Community

11th Security of Supply Coordination Group meeting
Ljubljana, 19 September 2018

Cybersecurity in the Energy Community

❖ Cyber attacks in **Ukraine** electricity networks

- **December 2015** – three Oblenergo (DSO) systems compromised: **Prykarpattya** – switched off 30 SS (230.000 citizens) for a period of 6 hours; **Chernivtsi** and **Kiyv** to lower extent - imposed vast damage on systems and data
- **December 2016** – 330 kV Transmission SS **Kiyv North** SCADA system compromised causing blackout for 1/5 of Kiyv demand for one hour – advanced, automated malware, swappable, adaptable and universal, simultaneous threat to multiple systems

❖ NIS Directive - (EU) 2016/1148

- The ECS proposed adaptation and adoption of the NIS Directive (energy) in the Energy Community
- PHLG (March 2018) Conclusions:
    - Acknowledged the necessity to build cybersecurity capabilities and risk management and incident reporting culture in the Energy Community
    - ECS 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
    - Recommended to eliminate regulatory gaps and develop cooperation structures, certification framework and research and education programs

NIS Directive

- Objective: to achieve a high common level of security of network & information systems via:

1. Improved cybersecurity capabilities at national level;
2. Increased cross-border cooperation;
3. Reporting obligations (on risk management and incidents) for operators of essential services and digital service providers.

Cybersecurity in the Energy Community

❖ Recommendations (based on NIS Directive):

- Create a Cooperation Group between CPs and MSs
- 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 emergency response mechanism, *inter alia* through Title III or Title IV measures
- Step-up public-private cooperation in cybersecurity

Cybersecurity in the Energy Community

❖ Study on Cybersecurity in the energy sector of the Energy Community

- Timeline
  - DDL for tenders: 20 Sept 2018
  - Contract: cca. 17 Oct 2018
  - Delivery of results: max 10 months (cca. Aug 2019)
- Overview of activities

Assessment & overview

Proposals

- Activities, measures and institutions in the EnC to overcome existing regulatory gaps (intra-EnC and vis-à-vis the EU) to achieve minimum common framework
- Cooperation mechanisms & acts in the EnC
- Recommendations to align certification, research & training

Impact assessment

- On the implementation of the proposed measures
- Roadmap on the timing of activities

Cybersecurity in the Energy Community

❖ Study on Cybersecurity in the energy sector of the Energy Community

- Contracting Parties are invited to
    - Work closely with the consultant
    - Provide all the necessary data
    - Engage the relevant actors in the energy sector

Cybersecurity in the Energy Community

❖ Study on Cybersecurity in the energy sector of the Energy Community

- Objectives
  - Identify and assess key 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 the NIS Directive and the Directive on European critical infrastructure and provide an impact assessment of their implementation in the Energy Community
  - Propose the necessary measures to improve cybersecurity in Contracting Parties
  - Propose a model for regional cooperation in managing cybersecurity risks and reporting incidents as well as a common cooperation platform, common certification framework and common framework for research, education and training programmes
  - Explore the possibility for the participation of Contracting Parties in the work of the European Union Agency for Network and Information Security (ENISA).

Cybersecurity in the Energy Community

❖ Study on Cybersecurity in the energy sector of the Energy Community

- Task 1
  - Identify the current legal and policy framework and administrative and regulatory rules and environment including competent authorities and law enforcement authorities relevant for cybersecurity in the domain of energy. In particular assess:
    - ✓ National strategies related to cybersecurity
    - ✓ Resilience measures including crisis prevention, monitoring and notification of incidents
    - ✓ Security requirements applicable in the energy and dependent sectors
    - ✓ Mechanisms for cross-border incident and crisis management
    - ✓ Public-private initiatives related to cybersecurity and existing training and education programmes
  - Assess whether Contracting Parties have measures in place transposing the NIS Directive, the Directive on European critical infrastructure and the Directive on attacks against information systems
  - Assess whether Contracting Parties took measures to implement the Council of Europe Convention on Cybercrime
  - Identify the current institutional framework for enhancing cybersecurity (authorities, market participants, CSIRTs)
  - Identify the existing cross-border cooperation initiatives
  - Identify the ongoing projects and technical assistance related to improving the governance on cybersecurity
  - Identify existing cybersecurity standards and certification schemes in Contracting Parties
  - Identify existing education and training programmes related to cybersecurity
  - Identify cyber threats and risks to which Contracting Parties are exposed

Cybersecurity in the Energy Community

❖ Study on Cybersecurity in the energy sector of the Energy Community

- Task 2
  - Based on the analysis of Task 1, identify the legal and regulatory gaps, inconsistencies and diverging provisions in the Contracting Parties' existing legal, regulatory and institutional frameworks
  - Identify and prepare an overview of the gaps in cybersecurity standards between the Contracting Parties and standards applicable in the EU
- Task 3
  - Propose amendments, policies, measures, procedures and recommendations necessary to implement minimum common framework addressing cybersecurity of critical infrastructure in the Energy Community
  - Propose and assess the cooperation mechanisms in the Energy Community (criteria for the identification of large-scale cybersecurity incidents, cross-border cooperation, relevant actors and standard operating procedures)
  - Recommendations how to align certification schemes and procedures as well as research, education and training programmes
  - Impact assessment of the implementation of the proposed acts and measures in the Energy Community
  - Develop a roadmap with the timing of the implementation of the proposed provisions and measures

www.energy-community.org

NIS Directive (backup)

- 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
- 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