CEER Citizens' Q&A

CEER Cybersecurity Report on Europe's Electricity and Gas Sectors

26 October 2018

1 Why is cybersecurity so important in the energy sector?

CEER has observed the intensification of threats to and incidents affecting energy markets, deriving from the massive use of cyber-attacks against elements of the energy system. These have the potential to destabilise and/or damage energy markets and thereby have a considerable impact on civil society.

The attack on the electricity grid infrastructure of Ukraine, in December 2015, provoked a wave of concern among energy operators and EU governments, as well as European energy regulators. Energy National Regulatory Authorities (NRAs) were, from the beginning, involved in analysing and understanding the phenomena, and providing inputs for viable solutions, especially in the EU interconnected grid. CEER accepted the challenge to possibly contribute to the identification of viable solutions in order to mitigate this tangible risk: Such solutions should take into consideration the specific economic aspects of the phenomena and of the energy market, the technical specificities of the energy system as it is structured now, and the potential risk that a similar event, on a large scale, may pose to the larger European society. Beyond this, the wave of digitalisation in the energy sector creates additional risks which must be considered up-front before any investment is approved. All this will be confronted within the context of ongoing activities which aim to adapt the market to the deteriorating security conditions of the cyber space in which digitalised energy markets operate.

2 What does the report propose for achieving a more cyber secure energy market?

The report makes some recommendations which may be seen as a potential and open contribution of NRAs to the mitigation of concerns related to cybersecurity. They are summarised here:

- All parties interacting with the grid not included in the list of Operators of Essential Services should, nevertheless, aim to develop and apply cybersecurity standards and measures.
- NRAs should, as far as possible within their legal powers, proactively engage with energy stakeholders in order to encourage them to be in compliance with the Directive on Security of Network and Information Systems (NIS Directive) and provide support for transposing horizontal regulation into sector-specific best practices that may help with an effective implementation of that directive.
- The Clean Energy for All Europeans Package does provide opportunities for more tailor-made obligations for TSOs/DSOs/Suppliers in the electricity sub-sector, and, in order to be even more effective, it may need to be extended and adapted to the needs of entire value chain of the electricity sub-sector (e.g. to generation).

- NRAs may also want to/be required to monitor the cybersecurity related expenditure and the effects of those cybersecurity-related investments to the risk landscape of the energy system and of individual operators, particularly regulated entities.
- CEER and ACER can work to promote culture change in cybersecurity.
- Management in energy-sector entities, including NRAs, should provide clear guidance on potential and expected cybersecurity governance.
- TSOs/DSOs/suppliers should have a cybersecurity strategy and they should set clear and effective cybersecurity measures prior embracing new technologies.

3 What else does the report help citizens understand?

This report aims to analyse current regulation and examine its potential effects as well as the potential effects of the regulation nearing the end of the legislative process in the EU, principally, the Clean Energy for All Europeans Package.

The on-going legislative process in regard to the Clean Energy Package, which is expected to be completed by the end of 2018, may set the pre-conditions to achieve the recommendations provided in this report.

In addition, NRAs may contribute, within the boundaries of their own competencies, to finding the best economic solutions to foster the adoption of preventive and protective measures against cyber-attacks at all levels of the energy value chain, while trying to avoid over-regulation. In addition, still within their existing mandate, and having in mind the obligation to assure security of supply, NRAs may contribute by providing correct and timely information to other entities in the energy sector with legitimate cybersecurity needs for that information.

4 Why is this important for energy customers?

Cybersecurity threats aim to disrupt the proper functioning of the energy system, and in a worst-case scenario, to create massive adverse events (black-outs, lack of gas in pipelines, disruption of heating systems) in widespread areas. Applying a proactive prevention for similar phenomena allows the sector to fulfil its aim of promoting the highest level possible of security of supply such that citizens can keep having energy products delivered to their households with the expected quality of service. Finally, energy regulators want to ensure that money spent on cybersecurity by energy operators in the EU, particularly regulated monopolies, follows a prudent and structured approach, maximising the effect of the investment toward achieving the final goal of a cyber-secure energy market. At the same time, costumer tariffs should be affected by this new technological challenge to the smallest extent possible.