ENERGI FÖRETAGEN

Datum
2021-06-28

To ACER: Draft Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows

Swedenergy (Energiföretagen Sverige) is a non-profit industry and special interest organisation for companies that supply, distribute, sell, and store energy. Mainly electricity, heating, and cooling. Swedenergy monitors and promotes the interests of its members and the Swedish energy sector in general. The organisation has a total of 400 members, which includes state-owned, municipal, and private companies as well as associations within the energy sector.

Key summary

- The Energy sector face multiple new targets for managing controls and meeting new security requirements that must be coordinated both by EU and in a national manner by authority according to requirements as the up-coming NIS-2 and Cybersecurity Act as well as this new regulatory instrument. The regulations must be coherent and streamlined to each other as far as taxonomy and methods are concerned.
- The compliance is typically enacted to protect information systems and sensitive data. However, since they frequently evolve to promote equal competitiveness between European countries according to information technology, industry influences and new threats to systems and data. Swedenergy proposes an approved national methodology for risk assessments for clarification of critical processes for the OT environment for increased delivery security. We also see need of clarification on security requirements for especially OT processes.
- We are of the view that the notion of “essential electricity undertaking” in the Framework Guidelines or other equivalent denomination (e.g., “essential business process in the Recommendations of the informal editorial or “cross-border electricity flows” in the Clean Energy Package) that determines the applicability of the network to an electricity undertaking should be defined entirely in the network code, not within the cross-border risk assessment process under Section 3 of the FG.
- Swedenergy recommend that the “size cap” for micro and mini and advanced would be reconsidered. The number of employees is not a relevant measure, not number of customers either. A relevant measure for producers also must be defined if they are to be subject to the code. One obvious solution is to leave the definitions of micro, mini and advanced to national regulators, knowing the functioning of the local market. In Sweden we have about 160 DSOs and most of them have less than 50 employees. Together they can have an impact on the cross border cyber security. Therefore, it is so important to identify critical/essential business processes even for small DSOs to perform the risk assessment at least in the level 1 (local).

Energiföretagen Sverige - Swedenergy - AB
101 53 Stockholm, Besöksadress: Olof Palmes Gata 31
Tel: 08-677 25 00, E-post: info@energiforetagen.se, www.energiforetagen.se
Org. nr: 556104-3265, Säte: Stockholm

- Our concern is that rules on cyber-security will be defined in the network code, but its scope of applicability will remain unclear until either (i) development and implementation of a methodology on risk assessment and defining Electricity Cybersecurity Risk Index (ECRI) or (ii) transitional measures are adopted by the ENTSO-E / EU-DSO working group. This representants significant uncertainty for the electricity undertakings. Swedenergy believe that it is important to set requirements based on functionality and processes.

- The risk assessments included in the processes are strongly regulated by national law which prevents such information from being reported. Swedenergy recommend therefore a top-down approach.

- There are doubts about the accountability of the process foreseen by the FG. While the cross-border risk assessment process under Section 1.5 and Section 3 is more inclusive than the transitional process under Section 1.6 none of the two processes guarantee due accountability. The cross-border risk assessment report will determine obligations of electricity undertakings; however, it is not subject to any regulatory or judicial review. Section 3.5.1 in point 13 indicates that the role of the Commission in the process will be limited to provide an opinion.

- Swedenergy recommend that the network code either defines the scope of applicability directly – by listing the electricity undertakings that fall within the scope or indirectly – through setting a methodology determining the applicability. Delegating the competence to define the scope of applicability through an implementation process is likely to result in uncertainty and accountability issues. Please keep in mind the lengthy and complex process of implementing the Network Code Balancing.

- Please consider changing the name “essential service supplier” to “essential service provider”, “digital service provider” or “vendor” as the term “supplier” can be confusing in the electricity context.

- Swedenergy proposes voluntary certification on essential products and not mandatory requirements. Product and measurements certifications are very far-fetched and may potentially result in limiting the availability of ICT products on the market and restrain innovation. At the same time, the measures foreseen by the FG do not include measures that are easier to apply: introducing basic level of security for services and products, long-term security patches or standard contractual clauses that would improve the situation of electricity undertakings vis-à-vis the vendors.

- Swedenergy believes that it is important to set requirements based on functionality rather than based on architecture instead of a mandatory SOC service at each company. We propose a HUB for incident reporting where the main responsibility is placed with ENTSO-E. A simple reporting according to ability increases the confidence of the industry to easily report. It would be helpful for a rapid reporting that is crucial.

- Requirements should be made on the functionality of delivery security with monitoring, measures, and actions. There are several key measures to follow that

help lower the risks of breaches and keep company's data safe despite the size of the company. The draft suggests four steps summarized below:

1. Thoroughly examine and determine where security risks lie in your organization through Electricity Cybersecurity Risk Index (ECRI).
2. Educate and communicate with decision makers in the organization and employees to help them understand how they can help close the gaps.
3. Implement the right tools that continuously and identify vulnerabilities as well as alert employees so that your organization can act quickly to reduce the risks.
4. Implement foundational controls and basic security hygiene. Monitor, measure and report compliance with security and privacy requirements.

- The Security Operation Centre (SOC): we agree with the objectives of the network codes on information sharing, smooth incident response or automated structuring of information sharing, however we are concerned about fixing all these functions to SOCs. The network code should foresee capabilities and functionalities of the electricity undertakings necessary for information sharing, however it should not prescribe the SOC as the one and only tool for such sharing. Even the small and micro enterprises should have a responsibility to share technical information and it must go hand in hand with a responsibility to monitor and detect intrusions. Grid participants must be obligated to identify risks and to detect threats even if they do not have the capability to run a SOC.

- A clear definition is needed when incidents are to be reported, as well as when feedback is given from CSIRT. The use of a standardized common taxonomy for cyber incidents as Mitre ATT&CK framework would support a rapid and stringent reporting. This allows the recipients of the shared information, to be clear what kind of threat it is.