Elektrotechnik & Informationstechnik (2017) 134/1: 14–18. DOI 10.1007/s00502-017-0473-7

European provisions for cyber security in the smart grid – an overview of the NIS-directive

M.-T. Holzleitner, J. Reichl

Due to increasing cyber-criminal actions security incidents pose a significant threat for society and economy. Such incidents may also affect personal data which could especially concern the exercise of economic activities, produce financial losses and harm the confidence of the users. To ensure the communication of the most serious security incidents there is a need to introduce minimum security requirements at Union level which apply to all communication and information systems. According to this risk the Network and Information Security Directive (NIS-Directive) (directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, Directive (EU) 2016/1148) entered into force in August 2016. But how will this Directive influence the Energy Sector – this question is being examined.

Keywords: NIS-Directive; Smart Grid; Smart Metering; Legal provisions; energy sector; national implementation

Rechtliche Aspekte von Cyber Security im Smart Grid – ein Überblick über die NIS-Richtlinie.

Wegen zunehmender Cyber-Kriminalität stellen Sicherheitsvorfälle eine erhebliche Bedrohung für Gesellschaft und Wirtschaft dar. Angriffe und Vorfälle können die Integrität und Übertragung personenbezogener Daten sowie geschäftlicher Informationen gefährden und dadurch die wirtschaftliche Entwicklung potenziell beeinträchtigen, was zu finanziellen Verlusten und der Gefahr des Vertrauensverlustes in die Informations- und Kommunikationstechnologie (IKT) im Allgemeinen führt. Als allgemeiner Ansatz für alle Sektoren, die in hohem Maße von der IT-Infrastruktur abhängen, wurde nach drei Jahren Verhandlungszeit die Richtlinie über Netz- und Informationssicherheit (NIS-Richtlinie) als erste Rechtsvorschrift zur Bewältigung der Herausforderung der Cyber-Sicherheit auf EU-Ebene verabschiedet. Die NIS-Richtlinie legt einen gemeinsamen EU-Ansatz für die Sicherheit des Internets fest und schreibt Betreibern kritischer Infrastrukturen bestimmte Pflichten vor. Die Bestimmungen sind jedoch generisch und nicht speziell für den Energiesektor konzipiert, weshalb die Vorgaben genauer in Bezug auf den Energiesektor untersucht werden.

Schlüsselwörter: NIS-Richtlinie; Energiesektor; Smart Grid; Stromnetz; Internetsicherheit; IKT

Received November 17, 2016, accepted December 13, 2016, published online January 24, 2017

1. Introduction

Experts predict cyber-criminal activities to become a major threat for society and economy in the future, if no appropriate measures are taken to counteract them. Attacks and incidents may affect the integrity and transfer of personal data and business related information, and thereby potentially hamper economic development, leading to financial losses and corrupting the confidence in information and communication technology (ICT) in general. To address these concerns, minimum security requirements at a European Union level shall ensure the security of all communication and information systems. A joint approach to tackle the risk of cyber-attacks is the new "Directive concerning measures to ensure a high common level of network and information security across the Union" (NIS-Directive)[1] that was published in the Official Journal of the EU on the 19th of July 2016[2] with the ambition to increase the level of Cyber-Security within the Member States. The NIS-Directive sets new security standards designed to ensure the security of critical network and information systems in central sectors of the economy like banking, energy, health and transport. The objective of the NIS-Directive is to improve and ensure the security of the internet, private networks and information systems.

The NIS-Directive came into force on 8th of August 2016, but is not immediately applicable for Member States. Member States have 21 months to transpose the NIS-Directive into national law, which means it will be implemented by the 10th of May 2018 across the EU. So by 11th of May 2018 the Directive becomes applicable for "Operators of Essential Services" and "Digital Service Providers", which are the two addressees falling under the provisions of the Directive.[3]

[1] Directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, Directive (EU) 2016/1148.

[2] Official Journal of the EU L 2016/194/1.

[3] The two terms "operators of essential services" and "Digital service providers" will be explained later on in the paper.

This paper is an outcome of the SPARKS project (project-sparks.eu) which has received funding from the European Unions's Horizon 2020 research and innovation programme under the grant agreement No. 608224.

Holzleitner, Marie-Theres, Energieinstitut an der Johannes Kepler Universität Linz, Altenberger Straße 69, 4040 Linz, Österreich (E-mail: Holzleitner@energieinstitut-linz.at); **Reichl, Johannes,** Energieinstitut an der Johannes Kepler Universität Linz, Altenberger Straße 69, 4040 Linz, Österreich

Network and Information Systems and Services play an essential role in society. Their reliability and security is necessary for many economic and societal activities, for the functioning of the internal market and to facilitate cross-border movement of goods, services and people. A network and information system is defined in the Directive as an electronic communications network. A network and information system means any device which is pursuant to a program and which performs automatic processing of digital data; including every digital data which is stored or processed, retrieved or transmitted for the purposes of their operation, use, protection and maintenance.[4] Network and information systems can be affected by security incidents, which may be caused by human mistakes, natural events, technical failure or malicious attacks. These incidents may cause a stop of business functioning, generate substantial financial losses for the EU economy or negatively affect societal welfare. Concerning these threats, it is really very important to adopt appropriate measures to secure network and information systems.

So, the aim of the Directive is to ensure a high common level of network and information security, to improve the security of the internet and private network and information systems, to increase preparedness of Member States, and to improve cooperation between the Member States.

The Directive defines six main objectives which have to be adopted by the Member States:

- Every Member State has to adopt a national NIS Strategy
- A cooperation group has to be created to support and facilitate strategic cooperation among Member States and to exchange information
- A Computer Security Incident Response Team network has to be created to focus operational cooperation and to work for confidence and trust between Member States
- Every Member State has to establish security and notification requirements for operators of essential services
- Every Member State has to establish security and notification requirements for digital service providers
- Every Member State has to designate three new national institutions: national competent authorities, single points of contact, and Computer Security Incident Response Teams (CSIRTs). These three institutions have to be tasked with security of network and information systems.[5]

According to a consultation on "Improving NIS in the EU[6]" made by the Commission, it could be determined that the energy sector is the second most important service to be affected by NIS requirements (directly after the banking and finance sector).[7] Despite that, the Directive is defined as a common regulation for all network and information systems, but does not specifically address the energy market nor the vital and ICT intensive subdomain thereof: the smart grid. However, considering the significant impact a disruption of energy supply would have on the economy and society,[8] a dedicated regulation may be required to comprehensively address the specific conditions of the energy market and its importance. Such specific regulation may be required, as most energy networks (in particular smart grids as part of electricity distribution networks) represent natural monopolies and the level of cyber security thereof is considered a (semi-)public good. In this context, this means that consumers have no possibility to satisfy their demand through the one smart grid offering the best price-security trade-off for their individual requirements, and thereby have low power to signal their preferred security level to the responsible entities. Additional motivation for a dedicated regulation arises from the criticality of an incident: the damage costs experienced by the smart grid operator in case of an incidence may be significantly lower than those of the affected society and economy, possibly leading to biased decisions when it comes to choosing the right level of investments into a networks' cyber security when left unguided through regulation.

2. Applicability

The Directive applies for Operators of Essential Services and Digital Service Providers, which are defined in the next subsection. However, it does not apply for sectors which are regulated separately in other provisions with at least equivalent requirements. This could mean that the Commission has planned the future development of regulations for specific sectors, like the Energy Sector.[9] Concerning Digital Service Providers, those requirements should not apply to micro- and small enterprises. In the author's opinion, the reason for this decision may just be that the required security measures may impose disproportionate burdens for those providers. However, if those small and micro digital service provider or any enterprise which is not listed as affected by the Directive would be part of a "future European Grid", those missing security standards could certainly cause major problems. This means that national provisions have to ensure that each enterprise connected to a grid has to follow minimum security requirements, irrespective of its size.

It is up to the national authorities to define the organisations which are considered by the national cyber security law. National authorities have to decide whether they define a list with information processes to inform the organisations concerned or to define a specification which means that the concerned organisations have to judge themselves if they are considered.

In any event, operators or providers for whom the Directive applies, have to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use for their operations or services.

2.1 Operator of essential services

An Operator of Essential Services is defined as a public or private entity which provides a service that is essential for the maintenance of critical and economic activities, and which depends on a network and information system. Furthermore, an incident on such service would produce a significant disruptive effect.[10]

Six months after national implementation of the NIS-Directive, every Member State has to identify operators of essential services[11] and prepare a list of referred services.[12] Referring to this provision in

[4] Art. 4 (1) NIS-Directive.

[5] Art. 1 (2) lit a-e NIS-Directive.

[6] The online public consultation on 'Improving network and information security in the EU' ran from 23 July to 15 October 2012.

[7] COM (2013) [2], 48 final, 7.

[8] See e.g. European Commission (2016) [1]; *Schmidthaler/Reichl* (2016) [4].

[9] Anyhow, there is no hint for a special regulation by now.

[10] Art. 5 (2) lit a-c NIS-Directive.

[11] Out of critical sectors such as the energy sector, transport sector, banking sector, financial market infrastructure, health sector, drinking water supply and distribution and digital infrastructure.

[12] The referred list has to provide information about national measures which were used to identify an Operator of Essential Services, a list of entities which may provide such a service, the number of respective Operators identified per sector and thresholds to determine the relevant supply level in accordance with the number of users relying on that service.

the Directive, there will be the question if every Member State will define a conclusive list with all Operators of Essential Services which has to be updated every two years?

However, identified operators of essential services have to take appropriate security measures and to notify serious incidents to the relevant national authority. Those national measures are required to significantly decrease related risks. Measures can be of technical and organisational nature, and shall be appropriate and proportionate in relation to the addressed risk. It is also required to ensure security of network and information systems, which means that the measures should ensure a level of security of those systems appropriate to the risks. Furthermore it should be ensured that incidents can be handled which means that measures should prevent and minimize the impact of incidents on the IT systems used to provide the services.

In the Energy Sector, suppliers of electricity and gas, as well as electricity or gas distribution or transmission system operators are listed as types of operators of essential services in Annex II of the Directive. Furthermore gas storage system operators, liquefied natural gas system operators, companies responsible for the production, transmission, distribution, supply, purchase or storage of natural gas and operators of natural gas refining and treatment facilities are also considered as operators of essential services. Likewise are operators of oil transmission pipelines and operators of oil production, refining and treatment facilities, storage and transmission categorized operators of essential services.[13]

There are many players in the energy market in general and the smart grids environment, in particular, for whom it is not yet sure whether they may be identified additionally to the list as operators of essential services. Examples of such players are parties being responsible for balancing in the power grid, energy generators from renewable sources or metering operators.

2.2 Digital service providers

A Digital Service Provider is defined as any legal person that provides a digital service. The Directive mentions three types of Digital Services which follow the purpose of the Directive:

- Online Marketplace: a digital service that allows consumers and/or traders to conclude online sales and service contracts
- Online Search Engine: a digital service that allows users to perform searches of all websites or websites in a particular language on the basis of a keyword, phrase or other input and which returns links to related content
- Cloud Computing Service: a digital service that enables access to a scalable and elastic pool of shareable computing resources.[14]

However, a recital says that "hardware manufacturers and software developers" are not digital service providers. When examining the NIS-Directive in the context of smart grids, the question arises whether there is any Digital Service Provider in the smart grid environment.

If there would be any Digital Service Provider, it must be examined if, e.g., the Data Aggregator[15] may be defined as Cloud Computing Service.

[13] Cf. Annex II Sector 1 of NIS-Directive.

[14] Cf. Annex III of NIS-Directive.

[15] Means any party that provides data aggregation services to electricity suppliers. They aggregate data to be submitted into settlements, so that accurate values of what a supplier's customers have "taken" is allocated to the correct supplier to enable the accurate billing of that supplier for the energy their customers have used (source: http://www.tma.co.uk/services/data-aggregation/ from 20.09.2016).

3. NIS-strategy

Due to the lack of common requirements around Europe, minimum capabilities are needed. In the introductory Sect. 1 it was mentioned that every Member State has to adopt a national NIS-Strategy with the aim to achieve and maintain a high level of security of network and information systems.

This strategy has to include:

- Strategic objectives, priorities and governance framework
- Identification of measures on preparedness, response and recovery
- Cooperation methods between the public and private sectors
- Plans for awareness raising, training and education
- Research & development plans related to the NIS Strategy
- Risk assessment plan
- List of actors involve in the strategy implementation

Art. 7 requires the adoption of a national NIS-Strategy but does not include special provisions for the energy sector, which means that Member States have to decide on their own how (much) they include provisions (measures, cooperation methods, ...) for the energy sector in the national NIS-Strategy.

As a cooperation method Austria has already established a dedicated national platform for discussing cyber security issues for public services and critical infrastructure providers.[16]

It will be interesting if Member States establish concrete measures in their strategies and if general measures will be set or measures defined for each sector. However, there is also to be decided by each Member State if the strategy should only have a national view to Cyber Security, a Cross Boarder view or even an international view. The European Commission will also have to cope with the different advancements within Member States which means that the national NIS-Strategy may differ among the Member States.

4. National institutions

Every Member State has to establish three Cyber Security institutions and provide adequate technical, financial and human resources therefor. The three institutions (the Competent Authority, the Single Point of Contact, and the Computer Security Incident Response Team – CSIRT) are responsible for consulting, cooperating, and coordinating with the relevant law enforcement national authorities and data protection authorities. Member States may request help and assistance of the European Agency for Network and Information Security (ENISA).

4.1 Competent authority and single point of contact

Member States have to designate one or more national competent authorities to monitor the application of the Directive at a national level. The Competent Authority is to be notified in case of an incident.[17] After fixing one or more national competent authorities, the designation has to be made public in every Member State. In relation to the Energy Sector and the Smart Grid, it may be useful to designate one Competent Authority for each sector which would be in line with the Directive.

Member States will also designate a single point of contact, which will exercise a liaison function to ensure cross-border cooperation. In case of an incident, which may also affect other Member States, the Single Point of Contact is responsible to notify the other affected Member States. The single point of contact will also submit

[16] This platform is called "Cyber Security Platform Austria (CSP).

[17] Cf. Art. 8, par. 6 NIS-Directive.

a yearly report on received notifications to the Cooperation Group (see Sect. 5; the report shall include the number of notifications, the nature of each incident, the type of the respective security breach, seriousness/duration and action taken). Competent Authority resp. CSIRT will provide necessary information therefor.

4.2 Computer security incident response team

Member States will designate one or more Computer Security Incident Response Teams, which may reside within the Competent Authority. There may be established multiple CSIRTs (for each considered sector[18]). CSIRTs are responsible for monitoring incidents, providing early threat warnings, responding to incidents, and cooperating with the private sector. Within the CSIRT shall be ensured high availability of communications services by avoiding single points of failure. Therefore appropriate, secure and resilient communication and information infrastructure at national level is to be guaranteed for CSIRTs. Additionally, CSIRTs have to promote adoption and use of common or standardised practices for incident handling and risk-handling procedures, as well as incident, risk and information classification schemes.

Concrete tasks of CSIRTs have to be clearly defined and supported by national policy. A definition of who should define the tasks of CSIRTs is missing in the Directive. As the Directive suggests that the CSIRT is established within the Competent Authority and also that assistance of ENISA may be requested, it may be standing to reason that a Member State delegates this task to Members of CSIRTs themselves in consultation with the Competent Authority.

CSIRTs may also be informed in case of an incident. The one who detects the incident may decide whether to inform the Competent Authority or the CSIRT. CSIRTs have to be an effective, efficient and secure cooperation part of the transnational CSIRTs network (described below).

5. Transnational networks

There are also established two new transnational institutions: Cooperation Group and CSIRTs Network.

The objective of the Cooperation Group is to support and facilitate strategic cooperation between Member States and to exchange information. The Cooperation Group will be composed of representatives of Member States, the Commission and ENISA. It is not defined which persons of a Member State should participate in the Cooperation Group. In the author's opinion, it may be helpful if each sector is represented in the Cooperation Group through a dedicated expert, but this is not defined. The choice lies with national implementation of the Member States. The Cooperation Group will constitute in February 2017.[19]

Furthermore, the NIS Directive establishes a network of CSIRTs, in which a representative from each Member State must participate. The network's tasks include exchanging information about security incidents, providing Member States with support in addressing cross-border incidents, and exploring and identifying further forms of operational cooperation. The aim of the CSIRT Network is to develop trust and confidence between the Member States and to promote underlayed and effective cooperation. The CSIRT Network consists of representatives of national CSIRTs and CERT-EU,[20] as well as members of the Commission with the role of an observer. ENISA should act as secretariat and actively support the cooperation among the CSIRTs. This network lays down its own rules of procedure.

These two transnational institutions do not have any power to set compulsive measures for Member States. They can only prepare proposals in their report to the Commission. So these groups resp. networks only have exchanging character and may only make suggestions to the Commission.

6. Incident notification

One main aspect of the NIS-Directive is the compulsory notification of Cyber incidents. Both Operators of Essential Services and Digital Service Providers have to ensure the security of their networks and systems to promote a culture of risk management and ensure that serious incidents are reported to the Competent Authority or CSIRT, but Digital Service Providers have less strict provisions.

6.1 For operators of essential services

Operators of Essential Services will have to notify National Competent Authorities or the CSIRT whenever there is a "significant" impact on the provision of the operator's service. The "significance" is not defined precisely in the Directive, but there are a few parameters that can be used for determining the incident. For the decision whether an incident is significant or not, an Operator of Essential Services has to take into account the number of users that are affected by the disruption of the service, the duration of the incident and the geographical spread, with regard to the area affected by the incident. Furthermore they have to balance how critical the incident is for society and economy.

If the incident has significant impact on the continuity of the essential service, other affected Member States are to be informed without undue delay. The decision whether the other Member State is to be informed or not is to be taken by the Competent Authority of the respective national CSIRT.[21] The operator's security, commercial interest and confidentiality of the provided information shall be preserved. Informing the public on individual incidents by the notified authority is set as an option as it may be decided where public awareness is necessary to prevent an incident or to deal with an ongoing incident. Nevertheless, the public is to be informed only after consultation with the concerned Operator of Essential Services.

6.2 For digital service providers

Digital service providers will be required to notify incidents that have a "substantial" impact on the provision of a service they offer in the EU without undue delay. The "substantiality" of an incident will be determined by relevant factors which are quite the same criteria as for Operators of Essential Services. In addition to those factors, the extent of the disruption of the functioning of the service and the extent of the impact on economic and societal activities are taken into account. However, the duty to notify incidents will only apply to digital service providers if they have access to the information needed to assess the impact of an incident against the parameters referred to.[22]

Notification to other Member States by Competent Authority or CSIRT is deemed particularly appropriate when the incident concerns two or more Member States.

In any case, security and commercial interests of the Digital Service Provider and the confidentiality of the information provided should

[18] According to Annex II of NIS-Directive.

[19] European Commission – Fact Sheet "Directive on Security of Network and Information Systems" Brussels, 6 July 2016 [3].

[20] The Computer Emergency Response Team for the EU institutions, agencies and bodies.

[21] The one who receives the notification.

[22] Cf. 15 (4) NIS-Directive.

be preserved. An obligation to inform the public is foreseen as well where public awareness is necessary to prevent an incident or to deal with an ongoing incident. What differs from requirements applicable to operators of essential services is that informing the public may be decided where disclosure of the incident is otherwise in the public interest. Information can be disclosed not only by the national Competent Authority or CSIRT but also, where appropriate, by the authorities or CSIRTs of other Member States concerned, and even by the Digital Service Provider itself if so required. Before informing the public, the Digital Service Providers have to be consulted.

Under the Directive, Member States will also be required to implement and enforce penalties against critical infrastructure providers that fail to comply with the Directive's requirements.

The scope of such a contractual notification obligation and the mentioned parameters need to be further defined by each Member State in order to be practically usable. A number of questions arise in the context of incident notification, especially for the energy sector: each Member State will have to determine what is a significant impact on a smart grid? What is the preferred format of the information? When is criticality of an incident justifying informing the public – in case of a blackout, data theft or technical failure? What is the difference between a significant[23] or a substantial[24] impact? Furthermore, what is a significant impact on a smart grid with impact on the continuity of essential services of another Member State? Where to draw the line between commercial interest and confidentiality of an operator, and the interest of public in being informed? When is public awareness necessary to prevent an incident? How can the state of the art be ensured, validated and maintained?

[23]For Operators of Essential Services.

[24]For Digital Service Providers.

7. Conclusions

The NIS Directive introduces provisions to achieve an improved level of harmonisation across Member States for network and information security, but it is not yet clear how it will be implemented into national laws of the Member States. It will be seen if Member States introduce new laws dealing especially with the requirements of the NIS Directive or if Member States will include the required security regulations into existing laws. Therefore, in Austria has been established a dedicated taskforce under the leadership of the Austrian Federal Chancellery for drafting a national cyber security law encompassing all the issues discussed throughout this paper. An initial version for further discussion should be published January 2017.

Based on many unanswered questions around the NIS Directive, Member States have to take important decisions when implementing the Directive into national law. There have to be found appropriate regulations for the different sectors and established different sector-based institutions in each Member State. According to different advancement in several Member States differing legal provisions are required in each Member State. Those provisions should be able to set the same security standard in all Member States to finally reach the goal of harmonisation within the European Union.

References

1. European Commission (2016): Commission staff working document – Impact assessment, accompanying the document "Proposal for a regulation of the European Parliament and of the Council concerning measures to safeguard security of gas supply and repealing Council Regulation 994/2010". SWD(2016) 25.
2. European Commission (2013): Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union. COM(2013), 48 final.
3. European Commission (2016): Fact sheet "Directive on security of network and information systems".
4. Schmidthaler, M., Reichl, J. (2016): Assessing the socio-economic effects of power outages ad hoc. Comput. Sci. Res. Dev., 31, 157.

Authors

Marie-Theres Holzleitner
is a junior researcher at legal department of the Energy Institute at the Johannes Kepler University in Linz, Austria. She examines legal provisions facing new challenges in the energy sector. Currently, she is researcher in the Horizon 2020 project "Personal Energy Administration Kiosk application" (PEAKapp), and in the FP 7 project "Smart Grid Protection Against Cyber Attacks" (SPARKS). Together with her colleague she organized a policy maker workshop "Smart Grids Security Requirements: Economic, Legal and Societal Aspects" in the European Parliament, Brussels, Belgium.

Johannes Reichl
is an applied statistical researcher who develops advanced econometric methods while investigating the challenges facing society in the fields of energy and resource economics. Currently, he is the scientific coordinator and principal investigator of the Horizon 2020 project "Personal Energy Administration Kiosk application" (PEAKapp), a Task Manager of the Horizon 2020 project "Innovative Large Scale Energy Storage Technologies & Power-to-Gas Concepts after Optimisation" (STORE & GO), and is the Legal, Ethical, Privacy and Policy Issues (LEPPI) Officer in the FP7 project "Smart Grid Protection Against Cyber Attacks" (SPARKS). Furthermore, he was the vice-coordinator of the FP7 project "Securing the European Electricity Supply Against Malicious and Accidental Threats" (SESAME), and was the chief developer of the software package www.blackout-simulator.com. He has organised and moderated a number of high level policy maker workshops on energy related topics, such as the 2016 workshop "Smart Grids Security Requirements: Economic, Legal and Societal Aspects" in the European Parliament, Brussels, Belgium, and the 2012 workshop "Emerging Malicious Threats to Electricity Infrastructure: Awareness and Preparedness of Professionals in TSOs and National Security Agencies" in the European Commission, Directorate-General for Home Affairs, Brussels.