TaylorWessing

Renewable Energy Plants as Critical Infrastructure

Requirements for IT protection

Background

The German Federal Office for Information Security (BSI) has been warning of increased risks for renewable energy plants (RE plants) for some time and reported specific attacks, including a possible cyberattack on thousands of wind turbines in February 2022. In April 2022, the IT systems of Deutsche Windtechnik, which is responsible for the maintenance of wind farms, were attacked. Only recently in 2023/2024, there was a cyber attack on the German Energy Agency (DENA) and Enercity. The functionality of the energy supply is more dependent than ever on intact information and communication communication technology (ICT).

It is established by law when energy generation plants belong to the so-called critical infrastructure and thus have to fulfil special requirements with respect to IT protection. In the energy sector (power supply), critical infrastructures include generation plants whose installed capacity exceeds certain threshold values. With the lowering of the threshold values as of January 2022, less large RES plants are now also considered critical infrastructure.

With our guide „Renewable Energy Plants as Critical Infrastructure – Requirements for IT Protection“, we take up this increasingly important topic and answer the most important questions regarding energy and IT protection law.

RES Plants as Critial Infrastructure

The obligations for operators of critical infrastructures in the energy sector and the answer to the essential question of whether the generating facility in question is to be classified as critical infrastructure arise from a whole series of different laws and ordinances:

- BSIG (IT Security Act)
- BSI KritisV (Ordinance for Determining Critical Infrastructures)
- EnWG (Energy Industry Act)
- IT Security Catalogue of the BNetzA (Federal Network Agency)

The **BSIG** stipulates that critical infrastructures are facilities, equipment or parts thereof which, among other things, belong to the energy sector and which are of great importance for the functioning of the community because their failure or impairment would result in significant supply shortages or threats to public safety (Section 2 (10)). The BSI KritisV as an ordinance based on the BSIG is of particular importance. The ordinance uses qualitative and quantitative criteria to determine which infrastructures are considered critical.

In the energy sector (power supply), these include generating plants and plants or systems for the control/bundling of electrical power. Whether a power generating plant is considered critical infrastructure depends largely on whether the threshold values defined in Annex 1 Part 3 of the KritisV are exceeded. The thresholds were lowered significantly as of January 2022, which means that smaller RES plants also fall within their scope. Whereas a threshold of 420 MW previously applied, the threshold for generating plants is now a net nominal capacity of only 104 MW. This means that many onshore wind farms, solar parks and especially offshore wind farms fall within the scope of the KritisV. Generating plants capable of black start are subject to the KritisV regardless of the amount of installed capacity. For plants providing primary control power, the threshold is 36 MW.

Thresholds for generating plants according to BSI KritisV in MW

Installed net nominal power (electrical or directly with heat extraction connected electrical active power with nominal heat output without condensation share)	Installed net nominal capacity if the installation is contracted as a black start installation according to Section 3 (2) of the BNetzA decision of 20 May 2020, ref. no. BK6-18-249	Installed net nominal capacity if the system is pre-qualified for the provision of primary control reserve pursuant to Section 2 No. 8 StromNZV
104 MW	0 MW	36 MW

Operator of RES Plants

According to Section 1 (1) no. 2 KritisV, an operator is a natural or legal person who, taking into account the legal, economic and factual circumstances, exercises a **determining influence** on the condition and operation of an installation or parts thereof. The possibility to exert a determining influence is given to anyone who can independently control the facility or parts thereof without instructions, whereby the legal power of disposal usually goes hand in hand with actual control. When assessing the economic circumstances, it is decisive who can derive the economic benefit from the facility and who bears the economic risk. The operator status is determined by an **overall assessment** of the aspects mentioned above.

In principle, it is irrelevant for the status of operator if he uses third parties to operate the facility as long as it does not relinquish decisive influence over the critical infrastructure himself. Even if the actual control lies with a commissioned service provider, the determining influence usually remains with the original operator due to contractually agreed rights of instruction and control. However, the situation may be different if the service provider provides its services largely independently of instructions.

A plant can only have one responsible operator (principle of **operator identity**). This is to ensure that rights and obligations can be clearly allocated.

Information Security Requirements of Operators of Critical Infrastructure RES Plants

Pursuant to Section 11 (1b) EnWG, operators of energy plants that have been designated as critical infrastructure and are connected to an energy supply network are obliged to ensure adequate protection against threats to telecommunications and electronic data processing systems that are necessary for secure facility operation. Adequate protection exists if the **IT Security Catalogue pursuant to Section 11 (1b) EnWG** of the BNetzA is complied with and this has been documented by the operator. Accordingly, the implementation of an **information security management system (ISMS)** that meets the requirements of **DIN EN ISO/IEC 27001** is needed in particular. When implementing the ISMS, the standards **DIN EN ISO/IEC 27002 and 27019**, each in their respectively valid version, must also be taken into account. The operator is also obliged to prove the conformity of its ISMS by means of a certificate issued by an independent certification body accredited for the certification of the IT Security Catalogue at the German Accreditation Body (DAkkS). Compliance can be verified by the BNetzA. From 1 May 2023 at the latest, operators must also implement appropriate systems for the detection of attacks and prove this to the BSI for the first time on this date and every two years thereafter, Section 11 (1d), (1e) EnWG.

Verification and Reporting Obligations

First, the operator itself must prove compliance with the requirements of the IT Security Catalogue in the form of a certificate. Independently of this, the service provider must also meet certain security criteria, whereby proof is provided through an independent certification procedure. More detailed information can be found in the **notice of the BNetzA** on certification in accordance with the IT Security Catalogue Section 11 (1a) and (1b) EnWG in the case of operational management by third parties.

Pursuant to Section 11 (1c) EnWG, operators of energy plants that have been designated as critical infrastructure must report faults that have led to a failure or to a significant impairment of the functionality of the energy plant concerned, or significant faults that may lead to a failure or to a significant impairment of the functionality of the energy plant concerned, to the BSI **without delay** - i.e. without culpable hesitation - via the designated contact point. A malfunction is deemed to have occurred if the technology used can no longer fulfil its intended function properly or completely, or if an attempt has been made to influence it accordingly.

Registration and other Obligations

Operators of critical infrastructures are obliged to register the facilities they operate with the BSI and to designate a contact point, Section 8b (3) BSIG. Furthermore, it must be ensured that the operator can be reached via the contact point at all times. Registration must take place no later than the first working day after the plant has been classified as a critical infrastructure for the first time or again.

In principle, operators of critical infrastructures must notify the BMI of the planned first use of a so-called critical component (Section 2 (13) BSIG) prior to its use, Section 9b (1) BSIG. Critical components are only those that are specifically defined by law. So far, this notification requirement is mainly relevant in the area of telecommunications.

Fines for Non-Compliance with the above Obligations

In principle, violations of the BSIG can be punished with fines of up to 20 million euros; the EnWG provides for a fine of up to 5 million euros. Due to the graduated catalogue of sanctions, however, these amounts are only relevant for certain - particularly serious - violations, such as violations of certain enforceable orders of the BSI. In contrast, violations of the IT security and reporting obligations of Section 11 EnWG constitute administrative offences pursuant to Section 95 (1) nos. 2a, 2b EnWG, which can be punished with a fine of up to one hundred thousand euros, Section 95 (2) Sentence 1 EnWG. A violation of the registration obligation under section 8b (3) BSIG is punishable by a fine of up to five hundred thousand euros pursuant to section 14 (2) no. 5, (5) sentence 2 BSIG; failure to ensure that the contact point is accessible is punishable by a fine of up to one hundred thousand euros, section 14 (2) no. 6, (5) sentence 2 BSIG.

TaylorWessing

Summary

In principle, changes to the existing legal framework are to be expected, as the NIS2 Directive, EU-wide legislation on network and information security, came into force at European level on January 16, 2023. Member states must transpose the directive into national law by October 17, 2024.

In Germany, there is already a draft bill from the Federal Ministry of the Interior for the implementation of the NIS 2 Directive (NIS-2UmsuCG).

The NIS2 Directive is intended to increase the requirements for cyber security and to harmonise Member State requirements. In particular, there will no longer be sector-specific thresholds; instead, it will be primarily the field of activity of a company and its size (number of employees and annual turnover or balance sheet) that will determine whether it falls under the scope of the directive as a "essential" or "important entity". On the legal consequences side, the requirements for sufficient cyber security risk management are to be increased and the reporting obligations extended. Furthermore, the authorities will be granted extended powers.

However, in view of the threat of fines of up to 10 million euros or up to 2 % of the total worldwide turnover in the previous business year, companies should keep a close eye on further developments in order to be able to take the necessary steps for NIS2 compliance in good time.

Your Contacts

Dr. Paul Voigt, Lic. en Derecho, CIPP/E
Berlin
+49 30 885636-408
p.voigt@taylorwessing.com

Dr. Markus Böhme, LL.M. (Nottingham)
Duesseldorf
+49 211 8387-430
m.boehme@taylorwessing.com