National Cyber and Information Security Agency
Mučednická 1125/31
616 00 Brno – Žabovřesky
Company ID No: 05800226
Data box ID: zzfnkp3

File No:
350 - 747/2022
Reference No:
6548/2022-NÚKIB-E/350

Brno, 30. May 2022

WARNING

The National Cyber and Information Security Agency, with its registered office at Mučednická 1125/31, 616 00 Brno (hereinafter the "Agency"), pursuant to Section 12(1) of Act No 181/2014, on cyber security and on the amendment of related laws, as amended (hereinafter the "Cyber Security Act"), issues this

Warning

about a cyber security threat of the use of technology or software not originating from the states of the European Union, the European Economic Area, the Organisation for Economic Co-operation and Development or the North Atlantic Alliance for implementation of technologies enabling the required level of direct metering of types B, C1, C2 or C3 pursuant to Decree No 359/2020, on electricity metering.

The National Cyber and Information Security Agency has evaluated this threat as "High" – the threat is likely up to very likely.

JUSTIFICATION

1. On the basis of facts established in the exercise of its powers, as well as on the basis of the facts the Agency has been informed of by its domestic partners, the Agency has identified a cyber security threat associated with the use of technology or software not originating from the states of the European Union, the European Economic Area, the Organisation for Economic Co-operation and Development, or the North Atlantic Alliance to implement technologies enabling the required level of direct metering of types B, C1, C2 or C3 pursuant to Decree No 359/2020, on electricity metering, and is therefore issuing this Warning about this threat pursuant to Section 12(1) of the Cyber Security Act.

2. This Warning is issued based on a combination of the following knowledge and findings.

Timeframe and nature of the situation

3. Some obligated entities pursuant to the Cyber Security Act, specifically the electricity distribution system operators, must immediately start preparatory work to deploy technology

enabling the required level of direct metering of types B, C1, C2 and C3 pursuant to Decree No 359/2020 (hereinafter the "Decree on Electricity Metering"), which is a regulation implementing Act No 458/2000, on business conditions and the performance of state administration in the energy sectors and on amendments to certain other laws (the Energy Act), respectively Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (hereinafter the "Internal Electricity Market Directive"). Therefore, the deployment of these technologies is not only a consequence of technological development and the introduction of innovations, but it is a matter of adhering to the obligations imposed by European Union legislation.

4. The fact that this Warning draws attention to the existence of a cyber security threat to a particular sector does not mean that the threat related to using technology originating from outside the above-mentioned states is irrelevant for other sectors. However, based on all the information gathered, the Agency found that in relation to the energy sector this threat appeared to be likely up to very likely.

5. As the Decree on Electricity Metering stipulates that the implementation of technologies enabling the required level of direct metering of types B, C1, C2 and C3 pursuant to the Decree on Electricity Metering will be started on 1 July 2024, and all consumption points defined by the Decree must have this technology implemented by 1 July 2027, the distribution system operators must launch tender or procurement proceedings pursuant to Act No 134/2016, on public procurement, without delay. Information provided by the distribution system operators shows that they expect the period between the start of the tender proceedings and the first delivery to last at least 18 months, and they further expect trial operation to be conducted on a limited range of equipment. Considering the scope of the contracts (due to the total number of consumption points that need to be equipped with new equipment) and the terms associated with the tender proceedings, as well as the complexity of the whole process of implementing the new technology, it is necessary to start tender proceedings as soon as possible so that the technology is implemented within the deadline set by legislation.

6. The facts set out in points 3, 4 and 5 of this Warning thus reinforce the urgency of the threat to which this Warning is responding.

Significance and scope of the possible impacts if this threat materialises

7. The impacts of information security breaches in systems with technology enabling the required level of direct metering of types B, C1, C2 and C3 for ensuring electricity supplies in the Czech Republic would be incomparably higher when compared to the currently used electricity metering technology. It would also be significantly easier for a supplier of technology and software supporting the functionality of this technology to cause such impacts than with the current technology.

8. Possible impacts of security breaches in technologies enabling the required level of direct metering of types B, C1, C2 or C3 on ensuring electricity supplies include the following:

a. Influencing metering and sending erroneous data to the central office.

b. The disconnection of consumption points (for example through bulk commands from the central office). With some solutions, physical presence at the consumption point is required for its reconnection, meaning the reconnection of the consumption point will not be immediate. With other solutions, it is possible to reconnect the consumption point from the central office, however there may still be destabilisation of the transmission system in the case of repeated disconnections and reconnections.

c. When a mass disconnection of thousands of consumption points occurs, the stability of the transmission system can be disrupted, which can result in a blackout – not only at the level of consumption points, but at the level of the transmission system as a whole.

9. The above impacts are significant in terms of their potential scope (up to approximately 5.5 million electricity meters, and therefore consumption points) and are among the largest and most serious possible impacts on the normal operation of the Czech Republic and its energy security. For this reason, it is necessary to consider possible threats with the highest possible level of detail, something this Warning is intended to facilitate.

10. The power sector, especially its electricity supply sub-sector, ensures one of the vital functions of the state. The impacts of the manifestation of this threat will not remain isolated in the given sub-sector, but will trigger a domino effect through all other sectors of the economy as well as every single citizen of this country. A negative influence on the technologies ensuring the proper functioning of the electricity system in the Czech Republic could thus cause impacts comparable to the complete paralysis of the Czech economy and everyday life.

11. Ensuring energy security is also a strategic goal of the Czech Republic, as follows from the Security Strategy of the Czech Republic.[1] Considering the current situation in the energy sector, where factors such as the pursuit of more environmentally friendly management of natural resources and the energy-related consequences of the war in Ukraine are coming together, ensuring the safe operation of electric power transmission and distribution is even more important.

12. The deployment of the relevant technology will involve significant financial and capacity costs. Mitigating the risk associated with the manifestation of this threat only in the future would mean that these costs would be paid once again outside the period for which these expenditures were planned, and could thus be reflected in energy prices for end consumers. In addition, putting risky technology into operation and addressing its replacement only retrospectively could significantly jeopardize the proper transmission, distribution and supply of electric power to end consumers, as well as the energy security of the Czech Republic. It is therefore necessary to warn of the existence of this threat now, before the technology and software that pose a cyber security threat is purchased, in order to allow the energy companies

[1] Government of the Czech Republic; Security Strategy of the Czech Republic for 2015, page 7, available here: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

obliged to introduce the new technology to continue working with the identified threat and take it into account in their risk management processes.

Non-technical aspects of cyber security

13. Cyber security is not only about assessing the technical aspects of technologies used – it is also, for example, necessary to consider the non-technical aspects of the security of the technologies when selecting suppliers, i.e. to assess the trustworthiness of the suppliers and subcontractors (manufacturers) of the given technologies. The trustworthiness of the supplier is then directly reflected in the trustworthiness of the delivered technology, and determines the level of risk associated with the use of such technologies. There must be confidence in the supplier at both the level of the final design of the delivered solution (quality) and at the strategic (non-technical) level, while confidence in the business, legal and political environments in which the supplier operates is also relevant. The Agency has long pointed out this fact, one often neglected in practice, and has emphasized this fact most recently together with the Ministry of Industry and Trade, the Ministry of Foreign Affairs, the Security Information Service, the Office for Foreign Relations and Information and the Military Intelligence, as public-law representatives of the security community of the Czech Republic through the publicly issued Recommendation for Assessing the Trustworthiness of Technology Suppliers of 5G Networks in the Czech Republic[2]

14. The following states can be considered as having a trustworthy legal environment:

    a. States with democratically elected governments, which includes, inter alia, the existence of an independent opposition, free elections through which the current government can be replaced, and a functioning principle of checks and balances,

    b. States with independent judicial systems not subject to direct political interference, which respect binding rules, customs and the principals of the rule of law, such as the right to a fair trial, including respect for the presumption of innocence, the right to a public hearing and the right to be tried without undue delay,

    c. States with legal regulations and public policies governed by the principles of the rule of law and which are issued with regard to them,

    d. States which protect intellectual property,

    e. States which do not violate international law systematically or for a long period of time, and against which or against whose activities international and supranational organisations or alliances of which the Czech Republic is a member do not officially protest, for example in the form of a United Nations Security Council resolution or a restrictive measure of the Common Foreign and Security Policy of the European Union,

[2] Available here: https://www.nukib.cz/cs/infoservis/doporuceni/1801-doporuceni-pro-hodnoceni-duveryhodnosti-dodavatelu-technologii-do-5g-siti-v-ceske-republice/

f. States which maintain partnerships with the Czech Republic and do not carry out activities directed against the fundamental interests of the Czech Republic or its allies,

g. States which do not consider the Czech Republic a hostile state.

15. The legal environment of the states described in the previous point of this Warning can be described as generally trustworthy. The states of the European Union, the European Economic Area, the Organisation for Economic Co-operation and Development and the North Atlantic Alliance are a group of states with a trustworthy legal environment, and the threat of prioritizing state interests over customer ones in these states is thus significantly less likely. The Czech Republic is also a member of all these groupings and these are therefore its allied states in various areas, from economic to military cooperation. Thus, it is significantly less likely for a delivery originating in one of these states to have the effects described in point 8 of this Warning.

16. The untrustworthy legal environment of some states has a direct impact on the trustworthiness of the companies established in them and which are subject to such legal environment. Due to the untrustworthiness of the legal environment, it cannot be ruled out that the companies in question will be forced by the state to prioritise the interests of their state over the interests of their customers.

Threat assessment

17. The facts set out in the above points of this Warning increase the severity of the threat to which this Warning is responding. Considering how significant the impact of an information security breach would be on these technologies and the possibilities available to the suppliers of these technologies, it is essential that the threat described in the Warning be properly assessed by the obligated entities and that appropriate security measures be taken.

18. For the purposes of this Warning, 'technology enabling the required level of direct measuring of types B, C1, C2 or C3 pursuant to the Decree on Electricity Metering' means the entire chain of data measuring, transmission and processing, including the means of communication involved in this chain.

19. In relation to technologies enabling the required level of direct measuring of types B, C1, C2 or C3 pursuant to the Decree on Electricity Measuring, it is necessary, as stated in this Warning, to consider where the given technology comes from. The origin of the technology must then be taken into account as it relates to its development, production, assembly or service, where this technology is essential in terms of ensuring information security and ensuring the control and functionality of the technology.

20. The Agency is authorised to issue this Warning pursuant to Section 22(b) of the Cyber Security Act, which empowers it to issue measures. Pursuant to Section 11(2) of the Cyber Security Act, these measures include Warnings pursuant to Section 12 of the Cyber Security Act. The Agency shall issue a Warning pursuant to Section 12(1) of the Cyber Security Act if it learns, in particular as a result of its own activities or through an initiative of the national CERT operator

or from authorities with competence in cyber security abroad, of a threat to cyber security. Pursuant to Section 12(2) of the Cyber Security Act, the Agency shall publish such Warning on its website and notify it to the authorities and entities referred to in Section 3 of the Cyber Security Act.

21. The Agency is tasked with ensuring prevention in the field of cyber security pursuant to Section 22(j) of the Cyber Security Act. This preventive activity also includes the provision of information on identified threats in cyber security. However, if a threat is of an intensity that information about it cannot be covered through the Agency's usual preventive activities, the Agency is forced to issue, in accordance with the above, a Warning pursuant to Section 12 of the Cyber Security Act.

22. The Agency points out that the authorities or entities obligated to introduce security measures pursuant to the Cyber Security Act in connection with risk management pursuant to Section 5(1)(h)(3) of the Cyber Security Decree, shall take into account the measures pursuant to Section 11 of the Cyber Security Act in their risk assessment and risk management plan. One of these measures is a Warning pursuant to Section 12 of the Cyber Security Act. On the basis of the aforementioned facts, the Agency considers the threat in the statement of this Warning to be likely up to very likely. The authorities and entities obligated to implement security measures pursuant to the Cyber Security Act and that are also affected by this Warning (i.e. electric power distribution system operators) shall therefore assess this threat at the appropriate level, i.e. at the level High. In the event the obligated entity uses another method for risk assessment pursuant to point 5 of Annex No 2 to the Decree on Cyber Security, this threat must be assessed in accordance with this method at a comparable level as in the case of the procedure pursuant to Section 5(1)(d) of the Cyber Security Decree.

23. The Agency further points out that pursuant to Section 4(4) of the Cyber Security Act, the authorities and entities referred to in Section 3(c) through (f) of the Cyber Security Act shall take into account the requirements arising from security measures when selecting a supplier for their information or communication systems, and include these requirements in the contract they will conclude with the supplier. Taking into account the requirements arising from the security measures referred to in the first sentence to the extent necessary to comply with the obligations pursuant to the Cyber Security Act cannot be considered an unlawful restriction of economic competition or an unjustified obstacle to economic competition.

Karel Řehka
Director
National Cyber and Information Security Agency