National Cyber and Information Security Agency
Mučednická 1125/31
616 00 Brno – Žabovřesky
ID: 05800226
Data mailbox ID: zzfnkp3

File reference:
350 - 401/2022
Case No.:
3381/2022-NÚKIB-E/350

Brno, 21 March 2022

WARNING

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

warning

against a cyber security threat consisting of non-compliance with contractual obligations by suppliers of ICT services and products with significant ties to the Russian Federation.

The Agency rates the threat as High – the threat is likely to very likely.

In view of the high level of this threat, the Agency recommends the following steps to authorities and persons obliged under the Cyber Security Act:

1. Check whether they use ICT services or products within their systems that depend on suppliers with significant ties to the Russian Federation. A significant tie to the Russian Federation is indicated by:

   1.1. the Supplier is based in the Russian Federation or is dependent on supplies from the territory of the Russian Federation.

   1.2. the ICT product or service essential to the functionality of the managed or operated information or communication system is delivered through the supplier´s branch in the Russian Federation.

   1.3. development or production of the ICT product or service essential to the functionality of the managed or operated information or communication system is situated in the Russian Federation.

2. In this regard, also verify whether their significant suppliers, as defined in Section 2(n) of Decree No. 82/2018 Coll., on security measures, cyber security incidents, reactive measures, submission requirements in the field of cyber security and data disposal (hereinafter "Cyber Security Decree"), use ICT services or products dependent on suppliers with significant ties to the Russian Federation.

3. If these authorities and persons or their significant suppliers use ICT services or products dependent on suppliers with significant ties to the Russian Federation, contact the suppliers with significant ties to the Russian Federation to determine:

   3.1. Whether and how it has addressed the risk of the impact of sanctions and the risk of possible unavailability of relevant services as part of its business continuity management.

   3.2. If this possibility is not accounted for by the supplier in the business continuity management or the solution is not satisfactory in a given case, ask the supplier to ensure remedy.

   3.3. If a remedy under clause 3.2 is not possible, incorporate (given the increased threat of non-compliance with the contractual obligation) a procedure for interruption of the supply of that ICT service or product into its business continuity management and consider an alternative solution if possible.

GROUNDS

1. Based on the facts established in the exercise of its competence, as well as on the basis of the facts which the Agency has obtained from authorities exercising competence in the field of cyber security abroad, as well as from domestic partners, the Agency has come to the conclusion that a cyber security threat is posed by potential non-compliance with contractual obligations by suppliers of ICT services and products with significant ties to the Russian Federation, and therefore issues the following warning pursuant to Section 12(1) of the Cyber Security Act.

2. A combination of the following observations and findings led the Agency to issue this warning.

3. ICT services and products supplied by companies with significant ties to the Russian Federation may be materially affected in the current situation as a result of the adoption of significant economic sanctions against and by the Russian Federation.

4. The above-mentioned economic sanctions (e.g. significant restrictions on the import of strategic commodities to the Russian Federation, including certain ICT technologies, or the disconnection of the Russian Federation from the SWIFT system) may affect the performance of obligations by suppliers with significant ties to the Russian Federation directly or indirectly due to a number of possible scenarios. Below is a description of four selected scenarios.

5. The sanctions imposed by the Russian Federation on the European Union or the Czech Republic may consist in a state ban on the performance or non-renewal of contractual obligations towards companies established in the European Union or the Czech Republic. Similarly, sanctions imposed by other states on the Russian Federation may prevent companies with significant ties to the Russian Federation from performing their obligations vis-à-vis Czech organizations. In addition, the performance of the obligations of companies with significant ties to the Russian Federation may be prevented by the termination of the supply of ICT products and services by major multinational ICT companies, which are leaving the Russian technology and service market in great numbers. The unavailability of their services and products within the Russian Federation may prevent the provision and development of services and products by suppliers with significant ties to the Russian Federation. Sanctions

(imposed on the Russian Federation) have also triggered the departure of many ICT specialists from the Russian Federation who were involved in the development, production and other necessary processes of suppliers with significant ties to the Russian Federation.

6. The Agency´s competence to issue this warning is based on Section 22(b) of the Cyber Security Act, which empowers the Agency to issue measures. Pursuant to Section 11(2) of the Cyber Security Act, such measures include warnings under 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 detects a cyber security threat, in particular based on its own activities or on the initiative of the operator of a national CERT or from authorities conducting cyber security activities abroad. In accordance with Section 12(2) of the Cyber Security Act, the Agency shall publish the warning on its website and notify the authorities and persons referred to in Section 3 of the Cyber Security Act.

7. The objective of the Agency under Section 22(j) of the Cyber Security Act is to ensure prevention in the field of cyber security. This preventive activity also includes the provision of information on identified cyber security threats. However, if the threat is of such intensity that information about it cannot be covered by the Agency´s standard preventive activities, the Agency shall issue a warning under Section 12 of the Cyber Security Act in accordance with the above.

8. The Agency advises that authorities or persons that are obliged to implement security measures pursuant to the Cyber Security Act shall take into account the measures pursuant to Section 11 of the Cyber Security Act in the risk assessment and risk management plan within risk management pursuant to Section 5(1)(h)(3) of the Cyber Security Decree. One of these measures is a warning pursuant to Section 12 of the Cyber Security Act. Based on the above, the Agency believes that the threat described in this warning is likely to very likely. Authorities and persons who are obliged to implement security measures under the Cyber Security Act are therefore obliged to assess this threat at the appropriate level, i.e. the High level. Where the obliged person uses another method for risk assessment in accordance with paragraph 5 of Annex 2 to the Cyber Security Decree, the threat must be assessed using this method at a comparable level as would be the case under the procedure foreseen in Section 5(1)(d) of the Cyber Security Decree.

9. The threat notified hereby by the Agency is already defined and specified within the Cyber Security Decree, namely threat type 10 in Annex 3 to the Cyber Security Decree “failure of the supplier to perform a contractual obligation”. This threat, in its generic form, should therefore already be addressed by the authorities and persons obliged under the Cyber Security Act in their risk analyses and related processes. This warning determines the specific level of threat to suppliers whose reliability is affected by the current geopolitical situation – the military conflict between the Russian Federation and Ukraine.

10. The Agency further notifies that, under Section 4(4) of the Cyber Security Act, the authorities and persons referred to in Section 3(c) to (f) of the Cyber Security Act are obliged to take into account the requirements resulting from security measures when selecting a supplier for their information or communication system and to include these requirements in the contract they

conclude with the supplier. Reflecting the requirements resulting from the security measures referred to in the first sentence to the extent necessary to perform the obligations under the Cyber Security Act shall not be regarded as an unlawful restriction of or an unjustified barrier to competition.

Karel Řehka
Director
National Cyber and Information Security Agency