National Cyber and Information Security Agency
Mučednická 1125/31
616 00 Brno-Žabovřesky
Identification number (IČO): 05800226
ID data box: zzfnkp3

File number:
110-536/2018
Reference number:
3012/2018-NÚKIB-E/110

December 17, 2018, Brno

W A R N I N G

The National Cyber and Information Security Agency, registered office at Mučednická 1125/31, 616 00 Brno, pursuant to §12 paragraph 1 of the Act No. 181/2014 Coll. on Cyber Security and Change of Related Acts (Act on Cyber Security), as amended, issues this

w a r n i n g :

The use of technical or program tools of the following companies, including their subsidiary companies, poses a threat to the cyber security.

- **Huawei Technologies Co., Ltd., Shenzhen, People's Republic of China**
- **ZTE Corporation, Shenzhen, People's Republic of China**

R E A S O N I N G

1) On the basis of the facts found during the execution of its competence, the National Cyber and Information Security Agency (hereinafter referred to as "NCISA") has found that the use of the technical or program tools of the aforementioned companies poses a threat to the cyber security and therefore, pursuant to §12 paragraph 1 of the Act on Cyber Security, issues this warning.

2) NCISA's competence to issue this warning is embedded within the provisions of §22, b), of the Act on Cyber Security, which empowers it to issue measures. Pursuant to §11 paragraph 2 of the Act on Cyber Security, these measures also include a warning under §12 of the Act on Cyber Security.

3) This warning has been issued based on the following findings.

4) The legal and political environment of the People's Republic of China ("PRC") in which the companies primarily operate and whose laws are required to comply with, requires private companies to cooperate in meeting the interests of the PRC, including participation in

intelligence activities etc. At the same time, these companies usually do not refrain from such cooperation with the state; in this environment, efforts to protect customers' interests at the expense of the interests of the PRC are significantly reduced. According to available information, there is an organizational and personal link between these companies and the state. Therefore, this raises concerns that the interests of the PRC may be prioritized over the interests of the users of these companies' technologies.

5) The PRC actively promotes its interests in the territory of the Czech Republic, including a conduct of influence and espionage intelligence activities (see, for example, Security Information Service Annual Report for 2017).

6) The security community's findings on the activities of these companies in the Czech Republic and around the world, which are available to NCISA, raise reasonable concerns about the existence of potential risks in using the technical or program tools they provide to their customers in order to support the interests of the PRC.

7) The technical and program tools of the aforementioned companies are being supplied to the information and communication systems that are or may be of strategic importance from the national security standpoint. Disruption of information security, i.e. disruption of the availability, integrity, or confidentiality of information in such information and communication systems can have a significant impact on the security of the Czech Republic and its interests.

8) These facts, in their entirety, lead to reasonable concerns about possible security risks in the use of these companies' technologies. The degree of potential risk due to the possible impact of information security breaches on information and communication systems relevant to the state is not negligible.

9) NCISA points out that the authorities or persons required to implement security measures under the Act on Cyber Security in connection with risk management pursuant to §5 paragraph 1 h) article 3 of the Decree No. 82/2018 Coll. on Security Measures, Cyber Security Incidents, Reactive Measures, Cyber Security and Data Disposal Submission Requirements (Cyber Security Regulation) in risk assessment and risk management plan shall take into account measures pursuant to §11 of the Act on Cyber Security. One of these measures is also a warning pursuant to §12 of the Act on Cyber Security.

10) NCISA points out that the authorities or persons required to implement security measures under the Act on Cyber Security in connection with risk management pursuant to §4 paragraph 1 c) and paragraph 2 c) of the Decree No. 316/2014 Coll. on Security Measures, Cyber Security Incidents, Reactive Measures, and Cyber Security Submission Requirements (Cyber Security Regulation) shall take into account threats and vulnerabilities. With regard to the transitional provision in §35 of the Decree No. 82/2018 Coll. on Security Measures, Cyber Security Incidents, Reactive Measures, Cyber Security and Data Disposal Submission Requirements (Cyber Security Regulation), these are the administrators and operators of the Critical Information Infrastructure information systems and the administrators and operators of the Critical Information Infrastructure communication systems, in case these systems were designated before May 28, 2018, as well as the administrators and operators of important information systems that met the criteria before May 28, 2018.

11) NCISA further points out that, pursuant to §4 paragraph 4 of the Act on Cyber Security, the authorities and persons referred to in §3 c) to f) of the Act on Cyber Security are required to take into account requirements arising from security measures during the selection of a supplier for their information or communication system, and include these requirements in a contract concluded with the supplier. Taking into account the requirements arising from security measures under the first sentence to the extent necessary to meet the obligations under the Act on Cyber Security cannot be considered an unlawful restriction of competition or an unjustified obstacle to competition.

Otisk úředního razítka

Ing. Dušan Navrátil
Director
National Cyber and Information Security Agency