Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno-Žabovřesky
IČO: 05800226
ID datové schránky: zzfnkp3

Spisová značka:
110 - 536/2018
Číslo jednací:
3012/2018-NÚKIB-E/110

Brno, 17. prosince 2018

VAROVÁNÍ

Národní úřad pro kybernetickou a informační bezpečnost, se sídlem Mučednická 1125/31, 616 00 Brno, podle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů vydává toto

v a r o v á n í :

Použití technických nebo programových prostředků následujících společností, včetně jejich dceřiných společností, představuje hrozbu v oblasti kybernetické bezpečnosti:

- **Huawei Technologies Co., Ltd., Šen-čen, Čínská lidová republika**
- **ZTE Corporation, Šen-čen, Čínská lidová republika**

ODŮVODNĚNÍ

1) Na základě skutečností zjištěných při výkonu své působnosti dospěl Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB") k tomu, že použití technických nebo programových prostředků výše vyjmenovaných společností představuje hrozbu v oblasti kybernetické bezpečnosti, a proto podle § 12 odst. 1 zákona o kybernetické bezpečnosti vydává toto varování.

2) Pravomoc NÚKIB je pro vydání tohoto varování dána ustanovením § 22 písm. b) zákona o kybernetické bezpečnosti, které jej zmocňuje k vydávání opatření. Podle § 11 odst. 2 zákona o kybernetické bezpečnosti patří mezi tato opatření i varování podle § 12 zákona o kybernetické bezpečnosti.

3) K vydání tohoto varování vedla kombinace následujících poznatků a zjištění.

4) Právní a politické prostředí Čínské lidové republiky („ČLR"), ve kterém uvedené společnosti primárně působí, a jejímiž zákony jsou povinny se řídit, vyžaduje po soukromých společnostech součinnost při naplňování zájmů ČLR, včetně podílu na zpravodajských aktivitách aj.

Tyto společnosti se zároveň takové spolupráci se státem povětšinou nebrání; úsilí chránit zájmy zákazníků na úkor zájmům ČLR je v tomto prostředí značně sníženo. Podle dostupných informací existuje organizační a personální propojení mezi těmito společnostmi a státem. Uvedené tedy vytváří obavy, že zájmy ČLR mohou být stavěny nad zájmy uživatelů technologií uvedených společností.

5) ČLR na území České republiky aktivně prosazuje své zájmy včetně provádění zpravodajských aktivit vlivového i špionážního charakteru (vizte například Výroční zpráva Bezpečnostní informační služby za rok 2017).

6) Poznatky bezpečnostní komunity, které jsou NÚKIB dostupné, o aktivitách uvedených společností v České republice i ve světě vytváří důvodné obavy z existence potenciálních rizik při využívání technických nebo programových prostředků, které tyto společnosti poskytují svým zákazníkům, s cílem podporovat zájmy ČLR.

7) Technické a programové prostředky uvedených společnosti jsou dodávány do informačních a komunikačních systémů, které mají či mohou mít z hlediska bezpečnosti státu strategický význam. Narušení bezpečnosti informací, tedy narušení dostupnosti, integrity nebo důvěrnosti informací v takových informačních a komunikačních systémech může mít zásadní dopad na bezpečnost České republiky a její zájmy.

8) Tyto skutečnosti ve svém souhrnu vedou k důvodné obavě z možných bezpečnostních rizik při používání technologií těchto společností. Míra potenciálního rizika vzhledem k možnému dopadu narušení bezpečnosti informací u informačních a komunikačních systémů důležitých pro stát je nezanedbatelná.

9) NÚKIB upozorňuje, že orgány nebo osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti, v souvislosti s řízením rizik podle § 5 odst. 1 písm. h) bod 3 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) při hodnocení rizik a v plánu zvládání rizik zohlední opatření podle § 11 zákona o kybernetické bezpečnosti. Jedním z těchto opatření je i varování podle § 12 zákona o kybernetické bezpečnosti.

10) NÚKIB upozorňuje, že orgány nebo osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti, v souvislosti s řízením rizik podle § 4 odst. 1 písm. c) a odst. 2 písm. c) vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) zohlední hrozby a zranitelnosti. S ohledem na přechodné ustanovení v § 35 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) se jedná o správce a provozovatele informačních systémů kritické informační infrastruktury a správce a provozovatele komunikačních systémů kritické informační infrastruktury, pokud tyto systémy byly určeny před 28. květnem 2018, jakožto i o správce a provozovatele významných informačních systémů, u kterých došlo k naplnění určujících kritérií před 28. květnem 2018.

11) NÚKIB dále upozorňuje, že v souladu s § 4 odst. 4 zákona o kybernetické bezpečnosti jsou orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle zákona o kybernetické bezpečnosti nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

Národní úřad pro kybernetickou a informační bezpečnost -3-

Ing. Dušan Navrátil
ředitel
Národní úřad pro kybernetickou a informační bezpečnost