NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST

ROZHODNUTÍ

Č. j.: 625/2019-NÚKIB-E/210 Brno 11. března 2019

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „**Úřad**“) rozhodl o žádosti ze dne 14. února 2019 podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „zákon o svobodném přístupu k informacím“), kterou podal žadatel [redacted] (dále jen „žadatel“), takto:

I.

[redacted]

ODŮVODNĚNÍ:

[redacted]

[redacted]

[redacted]

Dále Vám Úřad v souladu s ustanovením § 4 a § 14 odst. 5 písm. d) zákona o svobodném přístupu k informacím částečně poskytuje požadovanou informaci, a to ve formě odpovědí na dotazy:

1. V jakém rozsahu a na co konkrétně používá (sw a hw) od společností Huawei /ZET státní správa?

   Úřad nevede evidenci zařízení a softwarů, které používají orgány státní správy.

2. Je pro Českou republiku hrozbou fakt, že řešení Huawei používají také tři dominantní telefonní operátoři?

   Dle § 12 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti“), prostřednictvím varování Úřadu upozorňuje na existenci hrozby v oblasti kybernetické bezpečnosti, na kterou je nutné bezprostředně reagovat. Dá se předpokládat, že hrozba se dotýká většiny povinných subjektů podle zákona o kybernetické bezpečnosti. Ty se na základě zmíněného varování musí hrozbou dále zabývat a zohlednit ji v analýze rizik, kterou tyto subjekty v souladu s požadavky zákona o kybernetické bezpečnosti a 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) (dále jen „ vyhláška o kybernetické bezpečnosti“), již pravidelně provádí.

   Varování tedy neznamená bezpodmínečný zákaz používání daných technických a programových prostředků. Samotné označení technických a programových prostředků určité společnosti za hrozbu, jak to Úřad ve svém varování učinil, znamená, že je nutné tuto hrozbu zvážit a rozhodnout o výši rizika, které z používání zmíněných technických nebo programových prostředků pro

konkrétní prostředí konkrétní organizace plyne. Dovolí-li to tedy výsledky analýzy rizik, lze uvedené technické nebo programové prostředky nadále používat.

3. Mohou být ohrožena data podnikatelů zapojených do elektronické evidence tržeb?

   Jak je již zmíněno výše, povinné orgány nebo osoby podle § 3 písm. c) až f) zákona o kybernetické bezpečnosti jsou povinny podle § 5 zákona o kybernetické bezpečnosti provádět analýzu rizik. Na základě vyhodnocení rizik potom výše uvedené subjekty zavádějí a provádějí bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti v souladu s § 4 odst. 2 zákona o kybernetické bezpečnosti. Bezpečnostní opatření jsou blíže specifikována ve vyhlášce o kybernetické bezpečnosti. V souvislosti s řízením rizik musejí podle § 5 odst. 1 písm. h) bod 3 vyhlášky o kybernetické bezpečnosti tyto subjekty zohlednit mimo jiné i opatření podle § 11 zákona o kybernetické bezpečnosti, tedy i varování vydané podle § 12 zákona o kybernetické bezpečnosti.

5. Navrhnete či doporučíte zrušení nebo úpravu EET? Nevystavuje se Česká republika v opačném případě negativním důsledkům plynoucích z porušení dohody o ochraně investic?

   Dle § 4 zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky, ve znění pozdějších předpisů, je vybírání daní, poplatků a cel v působnosti Ministerstva financí. Není v pravomoci Úřadu navrhovat změny právních předpisů v gesci Ministerstva financí. Úřad jako ústřední správní úřad pro oblast kybernetické bezpečnosti, může pouze navrhnout změnu zákona v jeho gesci. Změny ostatních zákonů může toliko doporučit, avšak pouze jen v oblasti svěřené působnosti, tedy zejména v oblasti kybernetické bezpečnosti. Úřadu nepřísluší hodnocení v otázkách týkající se ochrany investic.

POUČENÍ

Proti tomuto rozhodnutí lze podle ustanovení § 16 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, v návaznosti na § 152 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, podat ve lhůtě 15 dnů od jeho doručení rozklad, o kterém rozhoduje ředitel Národního úřadu pro kybernetickou a informační bezpečnost. Rozklad se podává prostřednictvím Národního úřadu pro kybernetickou a informační bezpečnost.

otisk úředního razítka

Mgr. Pavel Král
ředitel odboru právního
Národního úřadu pro kybernetickou
a informační bezpečnost

Obdrží:
[redacted], emailem a datovou schránkou

Vypraveno dne:
viz otisk razítka na poštovní obálce nebo časový údaj na obálce datové zprávy