

*Parlament České republiky*  
**POSLANECKÁ SNĚMOVNA**  
**2019**  
*8. volební období*

253.

**USNESENÍ**  
*výboru pro evropské záležitosti*  
*z 34. schůze*  
*ze dne 18. září 2019*

k doporučení Komise ze dne 26. 3. 2019 – Kybernetická bezpečnost sítí 5G /kód Rady  
8068/19, C(2019) 2335 v konečném znění/

---

Výbor pro evropské záležitosti Poslanecké sněmovny Parlamentu ČR po vyslechnutí informace ředitele odboru kybernetických a bezpečnostních politik Národního úřadu pro kybernetickou a informační bezpečnost Mgr. et Mgr. Václava Borovičky, po vyslechnutí zpravodajské zprávy posl. Františka Kopřivy a po rozpravě

**s c h v a l u j e** stanovisko, které je přílohou tohoto usnesení.

Ondřej Veselý v. r.  
ověřovatel

František Kopřiva v. r.  
zpravodaj

Ondřej Benešík v. r.  
předseda

## **Doporučení Komise ze dne 26. 3. 2019 – Kybernetická bezpečnost sítí 5G**

**C(2019) 2335 v konečném znění, kód Rady 8068/19**

- **Právní základ:**  
Dokument informační povahy.
- **Datum zaslání Poslanecké sněmovně prostřednictvím VEZ:**  
2. 4. 2019
- **Datum projednání ve VEZ:**  
25. 4. 2019 (1. kolo)
- **Procedura:**  
Není projednáváno legislativním postupem, jedná se o dokument nelegislativní povahy, který nepodléhá schválení v Radě a Evropském parlamentu. Procedura je ukončena jeho přijetím a předložením těmto institucím.
- **Předběžné stanovisko vlády (dle § 109a odst. 1 jednacího řádu PS):**  
Datované dnem 15. května 2019, doručené do výboru pro evropské záležitosti dne 5. června 2019 prostřednictvím systému ISAP.
- **Hodnocení z hlediska principu subsidiarity:**  
Hodnocení z hlediska principu subsidiarity se neuplatní, jedná se o dokument informační povahy.
- **Odůvodnění a předmět:**  
Doporučení reaguje na kontroverze spojené s podezřením, že dodávky síťových prvků pro síť 5G ze strany některých čínských firem mohou představovat bezpečnostní riziko. Čínské firmy naopak označují tato obvinění za kampaň v rámci obchodních sporů mezi Čínou a Spojenými státy. Doporučení konkrétní firmy nejmenuje a snaží se používat neutrální technický jazyk.
- **Obsah a dopad:**  
Doporučení se týká bezpečnostních standardů budovaných nebo plánovaných mobilních sítí páté generace, tzv. 5G. Podle doporučení měly členské státy začít diskutovat dané téma v rámci **Skupiny pro spolupráci** (orgán zřízený podle směrnice č. 2016/1148) do 30. dubna 2019, to se stalo 11. dubna 2019 upřádáním prvního jednání.

Pokud jde o úroveň jednotlivých členských států, Evropská komise doporučovala, aby provedly posouzení rizik jejich 5G infrastruktury do 30. června 2019. Na základě tohoto posouzení pak měly aktualizovat standardy bezpečnostních rizik s ohledem na síť 5G, popř. přijmout jiná bezpečnostní opatření, spočívající zejm. ve zpřísnění povinnosti dodavatelů zajistit síťovou bezpečnost, a především **stanovit podmínky zabezpečení sítí 5G a ty požadovat od podniků, usilujících o přidělení 5G frekvencí.**

Toto vnitrostátní vyhodnocení měly členské státy předat do 15. července 2019 Evropské agentuře pro kybernetickou bezpečnost (**ENISA**). Ta pak měla provést mapování rizik

specifických pro síť 5G. V návaznosti na toto mapování by měly členské státy ve spolupráci s ENISA provést mapování expozice celé EU proti kybernetickým hrozbám, v první fázi se zaměřením na 5G technologie používané v průmyslu a následně na ty ostatní. Přezkum expozice EU by měl proběhnout do 1. října 2019.

Skupina pro spolupráci by pak měla vyjít z výše popsaných národních bezpečnostních hodnocení a s nimi spojených osvědčených opatření, aby je následně použila pro vytvoření „**sady nástrojů**“, použitelných pro snížení kybernetických rizik v celé EU. „**Sada nástrojů**“ by měla být vytvořena do 31. prosince 2019. Měla by obsahovat dvě základní části: A/ soupis typů bezpečnostních rizik, a B/ soubor možných opatření (např. certifikace softwaru a hardwaru, popř. různé zkoušky apod.).

V návaznosti na výše popsané průzkumy Komise doporučuje členským státům zavedení systému **certifikace síťových prvků**, relevantního pro síť 5G. Tento systém certifikace by pak měl být zahrnut do podmínek pro podniky, ucházející se o budování sítí 5G podle směrnice č. 2002/20/ES. Následně by měly státy ve spolupráci s Komisí spolupracovat na vytvoření zvláštních bezpečnostních požadavků, vztahujících se na zadávání **veřejných zakázek** v souvislosti se sítěmi 5G – ty by měly obsahovat **širší povinnou certifikaci**, než bude požadována pro zařízení pořizovaná mimo veřejné zakázky.

Závěrem Komise doporučuje, aby s ní členské státy spolupracovaly na posouzení účinků tohoto doporučení s cílem stanovit do 1. října 2020 vhodné navazující kroky.

- **Stanovisko vlády ČR:**

Rámcovou pozici zpracoval Národní úřad pro kybernetickou a informační bezpečnost. Podle jeho informací dosud byly plněny výše uvedené termíny, probíhají jednání ve Skupině pro spolupráci. Úřad předmětné doporučení Komise vítá, zejm. kvituje zmínění strategického zájmu, včetně právních a politických souvislostí. **Na druhou stranu úřad nesouhlasí s certifikací síťových prvků pro síť 5G**, protože podle něj nemůže fungovat – tyto prvky podle úřadu často silně závisí na softwarovém řešení, které je často updatováno. Rychlý sled aktualizací přitom podle úřadu účinnou certifikaci znemožňuje, v praxi by bylo stejně nutné používat prvky v necertifikovaném stavu. Úřad proto dává přednost sledu opatření, v němž je omezená certifikace jen jedním z kroků vedle zkoumání dodavatelského řetězce a prostředí v zemi dodavatele.

- **Předpokládaný harmonogram projednávání v orgánech EU:**

Doporučení nepodléhá schválení ze strany Evropského parlamentu, bude ho ale projednávat výbor pro průmysl, výzkum a energetiku (ITRE, jde o gesční výbor) a dále zahraniční výbor (AFET), výbor pro vnitřní trh (IMCO) a výbor pro občanské svobody, spravedlnost a vnitřní záležitosti (LIBE). Doporučení bylo výborům přikázáno 25. července 2019.

- **Závěr:**

Výbor pro evropské záležitosti

1. **v í t á** doporučení komise (EU) 2019/534 ze dne 26. března 2019 – Kybernetická bezpečnost sítí 5G a **s o u h l a s í** s rámcovou pozicí vlády;
2. **z d ů r a z ň u j e**, že pokud dodavatel či subdodavatel technologií pro tvorbu 5G sítí pochází ze země, která není stranou mezinárodních dohod o ochraně dat nebo má ve svém právním řádu zakotvenu povinnost dodavatelů spolupracovat se zpravodajskými

organizacemi či jinými složkami státu původu, může se jednat o riziko kybernetické bezpečnosti;

3. **p ř i p o m í n á** opakovaná upozornění Bezpečnostní informační služby na špionážní aktivity Čínské lidové republiky na území ČR a varování Národního úřadu pro kybernetickou a informační bezpečnost před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation;
4. **z d ů r a z ň u j e** nutnost využívání otevřeného hardware od certifikovaného regionálního výrobce v rámci informačních infrastruktur členských států EU pro získání větší kontroly, a tím posílení bezpečnosti, a **p o d p o r u j e** financování jeho vývoje ze společných prostředků EU;
5. **d o p o r u č u j e** po vzoru Spojeného království či Finska zvážit publikaci analýzy rizik 5G sítí;
6. **p o v ě ř u j e** předsedu výboru pro evropské záležitosti, aby v rámci politického dialogu postoupil toto usnesení předsedovi Evropské komise.

Ondřej Veselý v. r.  
ověřovatel

František Kopřiva v. r.  
zpravodaj

Ondřej Benešík v. r.  
předseda