POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY

PARLAMENTNÍ INSTITUT

DOKUMENTY EU

Kybernetická bezpečnost sítí 5G

Informační podklad k doporučení Komise ze dne 26. 3. 2019 - Kybernetická bezpečnost sítí 5G

Podklad k dokumentu Rady č. 8068/19
září 2019
zpracoval: Radek Píša

AKTUÁLNÍ VYDÁNÍ:

Název: Kybernetická bezpečnost sítí 5G
Zpracoval: Píša, R.
Číslo: Podklad k dokumentu č. 8068/19
Datum: září 2019

Klíčová slova:
5G; mobilní sítě; Huawei

ŘADA: DOKUMENTY EU

Typ řady: interní
První vydání řady: říjen 2004
Frekvence vydání řady: nepravidelná
Zaměření: Informační podklady k dokumentům EU projednávaným VEZ
Jazyk: CZ
Vydavatel: Kancelář Poslanecké sněmovny, Sněmovní 4, 118 26 Praha 1

PARLAMENTNÍ INSTITUT plní úkoly vědeckého, informačního a vzdělávacího střediska pro Poslaneckou sněmovnu, její orgány, poslance a Kancelář Poslanecké sněmovny, pro Senát, jeho orgány, senátory a Kancelář Senátu. Naše činnosti a produkty uvádíme níže.

Oddělení všeobecných studií	**STUDIE** Srovnávací studie Analytické studie	**ODPOVĚDI NA DOTAZ** Stručné odpovědi na dotazy členů Parlamentu	**VYBRANÁ TÉMATA** Studie zpracované k aktuálním problematikám	**MONITORING** Vybrané hospodářské měnové a sociální ukazatele	**MIGRACE** Přehled aktualit v oblasti migrace za vybrané období
	PŘEHLED SZBP Společná zahraniční a bezpečnostní politika EU	**EUROZÓNA+** Přehled ekonomických událostí v EU	**PODKLADY** pro zahraničně politická jednání	**PŘEDNÁŠKY** pro zahraniční delegace, PS, Senát	
Oddělení pro evropské záležitosti	**STANOVISKA** kompatibility nevládních návrhů zákonů s právem EU	**KONZULTACE** k předkládaným vládním návrhům zákonů	**DOKUMENTY EU** Výběr z aktů a dokumentů EU zaslaných PS	**ZPRÁVY** Aktuální agenda v Bruselu	**PODKLADY** pro jednání výboru na mezinárodní úrovni
Oddělení komunikace a vzdělávání	**INFORMAČNÍ STŘEDISKO** Informace o činnosti Poslanecké sněmovny a prohlídky budov	**ECPRD** Spolupráce s Evropským centrem pro parlamentní výzkum a dokumentaci	**PŘEDNÁŠKY** pro Poslaneckou sněmovnu, pro školy, veřejnost	**INFORMAČNÍ MATERIÁLY** o fungování Poslanecké sněmovny, o legislativním procesu	**ZÁPISY** ze schůzí, seminářů, přednášek, kulatých stolů

DOPORUČENÍ KOMISE

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

- 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 sítě 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 upořádáním 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 sítě 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 sítě 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 sítě 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 sítě 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.

- Projednávání ve výboru pro evropské záležitosti PS PČR:
  Výbor pro evropské záležitosti PS PČR projednal dokument dne 18. 9. 2019 a usnesením č. 253 přijal tyto závěry:

  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.