DOPORUČENÍ

DOPORUČENÍ KOMISE (EU) 2019/534

ze dne 26. března 2019

Kybernetická bezpečnost sítí 5G

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 292 této smlouvy,

vzhledem k těmto důvodům:

(1) Komise uznala, že zavedení síťových technologií 5. generace (5G) je hlavním faktorem umožňujícím rozvoj digitálních služeb budoucnosti a prioritou v rámci strategie pro jednotný digitální trh. Aby bylo zajištěno, že Unie bude mít od roku 2020 infrastrukturu pro připojení, jakou potřebuje pro svou digitální transformaci, přijala Komise akční plán 5G ([1]).

(2) Sítě 5G budou stavět na stávající 4. generaci (4G) síťových technologií; umožní poskytování nových služeb a stanou se centrální infrastrukturou a hnací silou pro velké části hospodářství Unie. Po svém zavedení budou sítě 5G tvořit páteř pro širokou škálu služeb, které jsou nezbytné pro fungování vnitřního trhu a zachování a provoz životně důležitých společenských a ekonomických funkcí – jako jsou energetika, doprava, bankovnictví a zdravotnictví, jakož i průmyslové řídicí systémy. O digitální infrastrukturu a sítě 5G se také bude ve stále větší míře opírat organizování demokratických procesů, například voleb.

(3) Závislost mnoha kritických služeb na sítích 5G by vedla k tomu, že následky systematických a rozsáhlých narušení budou velmi závažné. V této době, kdy kybernetické útoky jsou stále častější a sofistikovanější než dříve, je proto zajištění kybernetické bezpečnosti sítí 5G pro Unii otázkou strategického významu.

(4) Vzájemná propojenost a mezinárodní povaha infrastruktur, o něž se opírá digitální ekosystém, a přeshraniční povaha příslušných hrozeb znamenají, že jakékoli významné zranitelnosti a/nebo kybernetické bezpečnostní incidenty týkající se sítí 5G, které se vyskytnou v jednom členském státě, by měly dopad na Unii jako celek. Proto by měla být přijata opatření na podporu vysoké společné úrovně kybernetické bezpečnosti sítí 5G.

(5) Členské státy potvrdily, že jsou potřebná opatření na úrovni Unie. Evropská rada ve svých závěrech ze dne 21. března 2019 uvedla, že se zájmem očekává doporučení Komise ohledně jednotného přístupu k bezpečnosti sítí 5G ([2]).

(6) Jedním z hlavních cílů by mělo být zajištění evropské suverenity při plném respektování evropských hodnot otevřenosti a tolerance ([3]). Zahraniční investice ve strategických odvětvích, akvizice kritických aktiv, technologií a infrastruktury v Unii a dodávky kritických zařízení mohou pro Unii znamenat také bezpečnostní riziko.

(7) Kybernetická bezpečnost sítí 5G má zásadní význam pro zajištění strategické autonomie Unie, jak je uvedeno ve společném sdělení „EU-Čína – Strategický výhled“ ([4]).

(8) Usnesení Evropského parlamentu o bezpečnostních hrozbách souvisejících se zvyšující se technologickou přítomností Číny v Unii rovněž vyzývá Komisi a členské státy k přijetí opatření na úrovni Unie ([5]).

(9) Toto doporučení se zabývá kybernetickými bezpečnostními riziky v sítích 5G a za tímto účelem stanoví pokyny, které se týkají vhodných opatření v oblasti analýzy a zvládání rizik na vnitrostátní úrovni, vypracování koordinovaného evropského posuzování rizik a zavedení procesu pro vytvoření společné „sady nástrojů“ obsahující osvědčená opatření k řízení rizik.

(10) K ochraně sítí elektronických komunikací je zaveden robustní právní rámec Unie.

([1]) COM(2016)588 final.
([2]) Závěry Evropské rady ze dne 21. a 22. března 2019.
([3]) Stav Unie 2018 – Čas evropské suverenity, 12. září 2018.
([4]) JOIN (2019) 5 final.
([5]) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//CS.

(11) Rámec Unie v oblasti elektronických komunikací ([6]) podporuje hospodářskou soutěž, vnitřní trh a zájmy koncových uživatelů a s evropským kodexem pro elektronické komunikace ([7]) sleduje další cíl týkající se připojení, který je vyjádřen v podobě výsledků: obecný přístup k pevnému a mobilnímu připojení s velmi vysokou kapacitou a jeho využívání pro všechny občany a podniky Unie při zajištění ochrany zájmů občanů. Směrnice 2002/21/ES požaduje, aby členské státy zajišťovaly zachování integrity a bezpečnosti veřejných komunikačních sítí a uložily povinnosti, které zajistí, že podniky zajišťující veřejné komunikační sítě nebo poskytující veřejně dostupné služby elektronických komunikací přijmou technická a organizační opatření k odpovídajícímu zvládnutí rizik pro bezpečnost sítí a služeb. Rovněž stanoví, že příslušné vnitrostátní regulační orgány mají pravomoc zajistit dodržování takových povinností, včetně pravomoci vydávat závazné pokyny.

(12) Směrnice Evropského parlamentu a Rady 2002/20/ES ([8]) navíc umožnuje členským státům připojit k obecnému oprávnění podmínky týkající se zabezpečení veřejných sítí proti neoprávněnému přístupu za účelem ochrany důvěrného charakteru sdělení v souladu se směrnicí Evropského parlamentu a Rady 2002/58/ES ([9]).

(13) Na podporu provádění těchto povinností zřídila Unie řadu orgánů pro spolupráci. Agentura pro bezpečnost sítí a informací (ENISA), Komise, členské státy a vnitrostátní regulační orgány vypracovaly technické pokyny pro vnitrostátní regulační orgány týkající se hlášení incidentů, bezpečnostních opatření a hrozeb a aktiv ([10]). Skupina pro spolupráci ustavená směrnicí Evropského parlamentu a Rady (EU) 2016/1148 ([11]) (dále jen „skupina pro spolupráci“) sdružuje příslušné orgány za účelem podpory a usnadňování spolupráce, zejména poskytováním strategického vedení pro činnosti sítě bezpečnostních týmů typu CSIRT, která na technické úrovni usnadňuje operativní spolupráci.

(14) Základní podpůrný nástroj na podporu jednotné úrovně bezpečnosti by měl poskytnout budoucí evropský rámec pro certifikaci kybernetické bezpečnosti ([12]). Měl by umožnit rozvoj systémů certifikace kybernetické bezpečnosti, které budou reagovat na potřeby uživatelů zařízení a softwaru souvisejících s 5G. Vzhledem k zásadnímu významu těchto infrastruktur by rozvoj příslušných evropských systémů certifikace kybernetické bezpečnosti pro výrobky, služby nebo procesy informačních a komunikačních technologií používané pro sítě 5G měl být bezprostřední prioritou. Na rozvoji těchto systémů certifikace by se měli aktivně podílet členské státy a účastníci trhu, mimo jiné poskytováním podpory pro definici specifických profilů ochrany pro sítě 5G.

(15) Neexistují-li harmonizované právní předpisy Unie, mohou členské státy formou vnitrostátních technických předpisů přijatých v souladu s právem Unie stanovit, že evropský systém certifikace kybernetické bezpečnosti by měl být povinný. Členské státy mohou rovněž využít evropské systémy certifikace kybernetické bezpečnosti v souvislosti se zadáváním veřejných zakázek a směrnicí Evropského parlamentu a Rady 2014/24/EU ([13]) a mohly by podpořit vytvoření mechanismů pomoci – například asistenčního centra – pro pořizování řešení v oblasti kybernetické bezpečnosti ze strany zadavatelů veřejných zakázek.

(16) Důležitým prvkem při zajišťování bezpečnosti sítí 5G je vysoká úroveň ochrany údajů a soukromí. I na úrovni Unie byla stanovena pravidla zajišťující bezpečnost zpracování osobních údajů, mimo jiné i v elektronických komunikacích. Obecné nařízení o ochraně osobních údajů ([14]) ukládá povinnost zpracovávat osobní údaje způsobem, který zajistí jejich zabezpečení, včetně ochrany před neoprávněným přístupem k osobním údajům a zařízení používanému ke zpracování a před jejich neoprávněným používáním. Směrnice o soukromí

([6]) Směrnice Evropského parlamentu a Rady 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice) (Úř. věst. L 108, 24.4.2002, s. 33) a příslušné zvláštní směrnice.

([7]) Směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace (Úř. věst. L 321, 17.12.2018, s. 36).

([8]) Směrnice Evropského parlamentu a Rady 2002/20/ES ze dne 7. března 2002 o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice) (Úř. věst. L 108, 24.4.2002, s. 21).

([9]) Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31.7.2002, s. 37).

([10]) https://resilience.enisa.europa.eu/article-13.

([11]) Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).

([12]) Návrh nařízení Evropského parlamentu a Rady o agentuře ENISA, Agentuře EU pro kybernetickou bezpečnost, a zrušení nařízení (EU) č. 526/2013 a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií („akt o kybernetické bezpečnosti“) (COM(2017) 477 final – 2017/0225 (COD)).

([13]) Směrnice Evropského parlamentu a Rady 2014/24/EU ze dne 26. února 2014 o zadávání veřejných zakázek a o zrušení směrnice 2004/18/ES (Úř. věst. L 94, 28.3.2014, s. 65).

([14]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

a elektronických komunikacích stanoví zvláštní pravidla pro ochranu důvěrného charakteru sdělení a ochranu koncového zařízení uživatelů. Rovněž ukládá poskytovatelům služeb povinnost přijmout vhodná technická a organizační opatření, aby zajistili bezpečnost svých služeb.

(17) Unie rovněž přijala nástroj, který ochrání kritickou infrastrukturu a technologie, například infrastrukturu a technologie používané v telekomunikacích, tím, že umožní členským státům prověřovat přímé zahraniční investice z důvodu bezpečnosti nebo veřejného pořádku a vytvoří mechanismus spolupráce, v jehož rámci si členské státy a Komise budou moci vzájemně vyměňovat informace a vznášet obavy související s konkrétními investicemi ([15]).

(18) Členské státy a provozovatelé v současné době podnikají důležité přípravné kroky k tomu, aby mohly být sítě 5G zavedeny ve velkém měřítku. Několik členských států vyjádřilo obavy ohledně potenciálních bezpečnostních rizik spojených se sítěmi 5G v souvislosti s prováděním postupů pro udělování práv na užívání pásem rádiového spektra určených pro sítě 5G ([16]) a prověřovalo opatření k řešení těchto rizik.

(19) Při řešení kybernetických bezpečnostních rizik v sítích 5G by měly být zohledněny jak technické, tak i další faktory. Mezi technické faktory mohou patřit zranitelnosti v oblasti kybernetické bezpečnosti, které mohou být zneužity k získání neoprávněného přístupu k informacím (kybernetická špionáž, ať z ekonomických či politických důvodů) nebo k jiným zlovolným účelům (kybernetické útoky zaměřené na narušení nebo zničení systémů a dat). Důležitými aspekty, které je třeba uvážit, by měla být nutnost chránit sítě během celého životního cyklu a nutnost zahrnout všechno příslušné vybavení, též ve fázích projektování, vývoje, pořizování, zavádění, provozu a údržby sítí 5G.

(20) Mezi další faktory mohou patřit regulační nebo jiné požadavky kladené na dodavatele zařízení informačních a komunikačních technologií. Posouzení významu těchto faktorů by muselo zohlednit mimo jiné celkové riziko vlivu třetí země, zejména v souvislosti s jejím modelem správy věcí veřejných, neexistenci dohod o spolupráci v oblasti bezpečnosti nebo podobných ujednání – například rozhodnutí o odpovídající ochraně – týkajících se ochrany údajů mezi Unií a dotčenou třetí zemí, nebo to, zda je dotčená země smluvní stranou mnohostranných, mezinárodních nebo dvoustranných dohod o kybernetické bezpečnosti, boji proti kyberkriminalitě nebo ochraně dat.

(21) Jako důležitý krok v rámci tvorby přístupu Unie ke kybernetické bezpečnosti sítí 5G by mělo být provedeno a dokončeno posouzení rizik na vnitrostátní úrovni. To by členským státům pomohlo přizpůsobit vnitrostátní opatření týkající se bezpečnostních požadavků a řízení rizik ve světle uvedeného posouzení.

(22) Měla by být zavedena koordinace, aby byla zajištěna efektivita opatření zaměřených na řešení těchto kybernetických hrozeb, opatření nezbytných pro řádné fungování vnitřního trhu a opatření na ochranu osobních údajů a soukromí.

(23) Vnitrostátní posouzení rizik by se měla stát základem koordinovaného posouzení rizik na úrovni Unie, které by sestávalo z mapování hrozeb a společného přezkumu, což by prováděly členské státy s podporou Komise a společně s Evropskou agenturou pro kybernetickou bezpečnost (ENISA).

(24) Skupina pro spolupráci by měla – se zohledněním posouzení rizik na vnitrostátní úrovni a na úrovni Unie – vytvořit „sadu nástrojů“, která by identifikovala typy kybernetických bezpečnostních rizik a možná opatření na zmírnění těchto rizik v oblastech, jako je certifikace, zkoušení a řízení přístupu. Měla by rovněž určit možná zvláštní opatření vhodná k řešení rizik zjištěných jedním nebo více členskými státy. Skupina pro spolupráci by měla využívat podporu ze strany Evropské agentury pro kybernetickou bezpečnost (ENISA), Europolu, Sdružení evropských regulačních orgánů v oblasti elektronických komunikací (BEREC) a Zpravodajského a informačního centra EU. Tato sada nástrojů by měla Komisi napomáhat při vypracovávání minimálních společných požadavků, které dále zajistí vysokou úroveň kybernetické bezpečnosti sítí 5G v celé Unii.

(25) Při přijímání opatření k řešení kybernetických bezpečnostních rizik by se měla brát v úvahu podpora kybernetické bezpečnosti prostřednictvím diverzifikace dodavatelů při budování jakékoli jedné sítě.

([15]) Nařízení Evropského parlamentu a Rady (EU) 2019/452 ze dne 19. března 2019, kterým se stanoví rámec pro prověřování přímých zahraničních investic směřujících do Unie (Úř věst L 79 I, 21.3.2019, s. 1.).

([16]) V roce 2019 jsou naplánovány aukce v alespoň jednom pásmu spektra v 11 členských státech: Belgii, České republice, Francii, Irsku, Litvě, Maďarsku, Německu, Nizozemsku, Portugalsku, Rakousku, Řecku. Na rok 2020 se plánuje dalších šest aukcí: v Litvě (jiné kmitočty), na Maltě, v Polsku, na Slovensku, ve Spojeném království, ve Španělsku. Zdroj: http://5gobservatory.eu/observatory-overview/observatory-reports/.

(26) Tímto doporučením by neměla být dotčena příslušnost členských států, pokud jde o činnosti týkající se veřejné bezpečnosti, obrany a národní bezpečnosti a činnosti státu v oblasti trestního práva, včetně práva členských států vyloučit ze svých trhů poskytovatele nebo dodavatele z důvodů národní bezpečnosti,

PŘIJALA TOTO DOPORUČENÍ:

I. **CÍLE**

1) Toto doporučení za účelem podpory vytvoření přístupu Unie k zajištění kybernetické bezpečnosti sítí 5G určuje činnosti, které by měly být uskutečněny, aby:

a) členské státy mohly posoudit kybernetická bezpečnostní rizika ovlivňující sítě 5G na vnitrostátní úrovni a přijmout nezbytná bezpečnostní opatření;

b) členské státy a příslušné orgány, agentury a jiné subjekty Unie mohly společně vypracovat koordinované posouzení rizik na úrovni Unie, které bude vycházet z vnitrostátního posouzení rizik;

c) skupina pro spolupráci ustavená podle směrnice (EU) 2016/1148 (dále jen „skupina pro spolupráci“) mohla určit možný společný soubor opatření, která by měla být přijata, aby se zmírnila kybernetická bezpečnostní rizika týkající se infrastruktur, o něž se opírá digitální ekosystém, zejména sítí 5G.

II. **DEFINICE**

2) Pro účely tohoto doporučení se rozumí:

a) „sítěmi 5G“ soubor všech relevantních prvků síťových infrastruktur pro mobilní a bezdrátovou komunikační technologii používanou pro připojení a služby s přidanou hodnotou s vyspělými výkonnostními charakteristikami, jako jsou velmi vysoká rychlost přenosu dat a kapacita, komunikace s nízkou latencí, mimořádně vysoká spolehlivost nebo podpora vysokého počtu připojených zařízení. Mohou zahrnovat starší prvky sítí založené na předchozích generacích mobilní a bezdrátové komunikační technologie, jako jsou 4G nebo 3G. Sítě 5G by měly být chápány tak, že zahrnují všechny relevantní části sítě;

b) „infrastrukturami, o něž se opírá digitální ekosystém“ infrastruktury, které slouží k tomu, aby umožnily digitalizaci v širokém spektru kritických aplikací v hospodářství a ve společnosti.

III. **ČINNOST NA VNITROSTÁTNÍ ÚROVNI**

3) Členské státy by do 30. června 2019 měly provést posouzení rizik infrastruktury sítí 5G, včetně určení nejcitlivějších prvků, kde by narušení bezpečnosti měla významný negativní dopad. Do téhož data by členské státy měly rovněž přezkoumat bezpečnostní požadavky a metody řízení rizik použitelné na vnitrostátní úrovni s cílem zohlednit kybernetické bezpečnostní hrozby, které mohou vyplynout z i) technických faktorů, jako jsou specifické technické vlastnosti sítí 5G, a z ii) jiných faktorů, jako je právní a politický rámec, který se může v třetích zemích vztahovat na dodavatele zařízení informačních a komunikačních technologií.

4) Na základě tohoto vnitrostátního posouzení rizik a přezkumu a s ohledem na probíhající koordinovanou činnost na úrovni Unie by členské státy měly:

a) aktualizovat uplatňované bezpečnostní požadavky a metody řízení rizik s ohledem na sítě 5G;

b) aktualizovat příslušné povinnosti uložené podnikům zajišťujícím veřejné komunikační sítě nebo poskytujícím veřejně přístupné služby elektronických komunikací podle článků 13a a 13b směrnice 2002/21/ES;

c) připojit k obecnému oprávnění podmínky týkající se zabezpečení veřejných sítí proti neoprávněnému přístupu a požadovat od podniků, které se účastní jakýchkoli nadcházejících řízení o udělení práv na užívání rádiových kmitočtů v pásmech 5G, závazky týkající se dodržování bezpečnostních požadavků na sítě podle směrnice 2002/20/ES;

d) uplatňovat jiná preventivní opatření zaměřená na zmírnění potenciálních kybernetických bezpečnostních rizik.

5) Opatření podle bodu 4 by měla zahrnovat přísnější povinnosti dodavatelů a provozovatelů zajistit bezpečnost citlivých částí sítí, jakož i v příslušných případech například povinnost poskytovat relevantní informace příslušným vnitrostátním orgánům, pokud jde o plánované změny v sítích elektronických komunikací, a požadavky, aby specifické komponenty a systémy informačních technologií byly předem zkoušeny vnitrostátními auditními/certifikačními laboratořemi z hlediska zabezpečení a integrity.

6) Měly by se provádět společné přezkumy bezpečnosti s účastí dvou nebo více členských států, při nichž budou využity a sdíleny příslušné technické odborné znalosti a zařízení týkající se infrastruktur, o něž se opírá digitální ekosystém, a sítí 5G, například pokud tentýž podnik provozuje nebo buduje síťovou infrastrukturu ve více než jednom členském státě nebo pokud jsou si konfigurace sítí velmi podobné. Evropská agentura pro kybernetickou bezpečnost (ENISA), Europol a Sdružení evropských regulačních orgánů v oblasti elektronických komunikací (BEREC) by měly upřednostňovat žádosti o podporu ze strany členských států v této oblasti. Výsledky těchto přezkumů by měly být předány skupině pro spolupráci a síti bezpečnostních týmů typu CSIRT.

IV. **KOORDINOVANÁ ČINNOST NA ÚROVNI UNIE**

7) S cílem vytvořit společný přístup k řešení kybernetických bezpečnostních rizik, pokud jde o sítě 5G, by členské státy měly do 30. dubna 2019 ve skupině pro spolupráci zahájit práci ve zvláštní oblasti činnosti. Členské státy by měly vyzvat příslušné orgány, aby se práce skupiny pro spolupráci v příslušných případech účastnily.

Koordinované evropské posouzení rizik

8) Členské státy by si měly mezi sebou navzájem a s příslušnými orgány Unie vyměňovat informace za účelem vytváření společného povědomí o stávajících a potenciálních kybernetických bezpečnostních rizicích spojených se sítěmi 5G.

9) Do 15. července 2019 by členské státy měly předat své vnitrostátní posouzení rizik Komisi a Evropské agentuře pro kybernetickou bezpečnost (ENISA).

10) Evropská agentura pro kybernetickou bezpečnost (ENISA) by měla provést mapování hrozeb specifické pro sítě 5G. Skupina pro spolupráci a síť bezpečnostních týmů typu CSIRT ustavené podle směrnice (EU) 2016/1148 by měly tento proces podporovat.

11) Členské státy by do 1. října 2019 a se zohledněním všech těchto prvků měly s podporou Komise a společně s Evropskou agenturou pro kybernetickou bezpečnost (ENISA) provést společný přezkum expozice celé Unie vůči rizikům souvisejícím s infrastrukturami, o něž se opírá digitální ekosystém, zejména se sítěmi 5G.

12) Tento společný přezkum by měl upřednostnit analýzu rizik, která se týkají zvláště citlivých nebo zranitelných prvků patřících mezi páteřní prvky sítí 5G, střediska provozu a údržby a přístupových prvků sítí 5G používaných pro průmyslové účely.

13) V druhé fázi by tento společný přezkum měl být rozšířen na další strategické prvky digitálního hodnotového řetězce.

Společná sada nástrojů Unie k řešení rizik

14) Skupina pro spolupráci by v rámci své činnosti měla určit osvědčená opatření typu uvedeného v bodě 4 uplatňovaná na vnitrostátní úrovni. Na základě těchto vnitrostátních osvědčených postupů by měla být do 31. prosince 2019 dohodnuta „sada nástrojů" sestávající z vhodných, účinných a přiměřených možných opatření k řízení rizik na zmírnění identifikovaných kybernetických bezpečnostních rizik na vnitrostátní i unijní úrovni, která Komisi poskytne poradenství k tvorbě minimálních společných požadavků k dalšímu zajištění vysoké úrovně kybernetické bezpečnosti sítí 5G v celé Unii.

15) Tato sada nástrojů by měla zahrnovat:

a) soupis typů bezpečnostních rizik, která mohou mít vliv na kybernetickou bezpečnost sítí 5G (např. riziko v dodavatelském řetězci, riziko zranitelnosti softwaru, riziko spojené s řízením přístupu, rizika vyplývající z právního a politického rámce, který se může v třetích zemích vztahovat na dodavatele zařízení informačních a komunikačních technologií), a

b) soubor možných zmírňujících opatření (např. certifikace hardwaru, softwaru nebo služeb třetími stranami, formální zkoušky nebo kontroly shody hardwaru a softwaru, procesy k zajištění existence a vynucování řízení přístupu, identifikace produktů, služeb nebo dodavatelů považovaných za potenciálně nezabezpečené atd.). Tato opatření by se měla zabývat všemi typy bezpečnostních rizik identifikovaných v jednom nebo více členských státech na základě posouzení rizik.

16) Jakmile budou vypracovány evropské systémy certifikace kybernetické bezpečnosti relevantní pro sítě 5G, měly by členské státy v souladu s právem Unie přijmout vnitrostátní technické předpisy, které stanoví povinnou certifikaci produktů, služeb nebo systémů informačních a komunikačních technologií, na něž se tyto systémy certifikace vztahují.

17) Členské státy by spolu s Komisí měly určit podmínky týkající se zabezpečení veřejných sítí před neoprávněným přístupem, které mají být připojeny k obecnému oprávnění, a bezpečnostní požadavky na sítě za účelem požadování závazků ze strany podniků, které se účastní řízení o udělení práv na užívání spektra v pásmech 5G podle směrnice 2002/20/ES. Tyto podmínky a požadavky by se měly pokud možno odrážet v přijatých opatřeních podle bodu 4 písm. c).

18) Členské státy by měly spolupracovat s Komisí na vypracování specifických bezpečnostních požadavků, které by se mohly uplatnit v rámci zadávání veřejných zakázek v souvislosti se sítěmi 5G. Měly by zahrnovat povinné požadavky na provedení systémů certifikace kybernetické bezpečnosti v zadávání veřejných zakázek, neboť tyto systémy certifikace nejsou dosud pro všechny dodavatele a provozovatele závazné.

V. **PŘEZKUM**

19) Členské státy by měly spolupracovat s Komisí na posouzení účinků tohoto doporučení do 1. října 2020 s cílem stanovit vhodné navazující kroky. Uvedené posouzení by mělo zohledňovat výsledky koordinovaného posouzení rizik na úrovni Unie a sadu nástrojů Unie.

Ve Štrasburku dne 26. března 2019.

Za Komisi
Julian KING
člen Komise