

Brusel 2. prosince 2020
(OR. en)

13629/20

CYBER 263
TELECOM 248
COPEN 362
CODEC 1266
COPS 441
COSI 235
CSC 344
CSCI 86
IND 248
RECH 493
SPACE 77

VÝSLEDEK JEDNÁNÍ

Odesílatel:	Generální sekretariát Rady
Datum:	2. prosince 2020
Příjemce:	Delegace

Předmět:	Závěry Rady o kybernetické bezpečnosti zařízení připojených k internetu – závěry Rady schválené písemným postupem
----------	--

Delegace naleznou v příloze závěry Rady o kybernetické bezpečnosti zařízení připojených k internetu, které Rada schválila písemným postupem dne 2. prosince 2020.

Závěry Rady o kybernetické bezpečnosti zařízení připojených k internetu

Rada Evropské unie,

PŘIPOMÍNÁJÍC:

- závěry Rady o společném sdělení Evropskému parlamentu a Radě: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU,
 - závěry Rady o budování kapacit a schopností v oblasti kybernetické bezpečnosti v EU,
 - závěry Rady o významu 5G pro evropské hospodářství a potřebě zmírnit bezpečnostní rizika spojená s 5G,
 - závěry Rady o budoucnosti vysoce digitalizované Evropy po roce 2020: „Posílení digitální a hospodářské konkurenceschopnosti v Unii a digitální soudržnosti“
 - závěry Rady o utváření digitální budoucnosti Evropy
 - závěry Evropské rady o pandemii COVID-19, jednotném trhu, průmyslové politice, digitálních aspektech a vnějších vztazích,
 - sdělení Evropské komise o utváření digitální budoucnosti Evropy,
1. **ZDŮRAZŇUJE**, že je třeba, aby si Evropská unie a její členské státy zajistily digitální suverenitu a strategickou autonomii, aniž by byla dotčena otevřená ekonomika. Tento cíl obnáší posílení schopnosti přijímat samostatná rozhodnutí ohledně technologií, jakož i existenci odolných a bezpečných infrastruktur produktů a služeb, jež představují jeden z hlavních pilířů v dané oblasti a díky nimž lze budovat důvěru v jednotný digitální trh i důvěru uvnitř evropské společnosti jako takové. Základní hodnoty Evropské unie jsou především zárukou zachování soukromí, bezpečnosti, rovnosti, lidské důstojnosti, právního státu a otevřeného internetu, což jsou nezbytné předpoklady pro vybudování společnosti, hospodářství a průmyslu, jež se budou opírat o digitální rozvoj a jež budou zaměřeny na člověka.

2. JE SI VĚDOMA vzrůstajícího významu zařízení připojených k internetu a jejich bezpečnosti, včetně strojů, senzorů a sítí, z nichž sestává internet věcí. Zařízení připojená k internetu hrají klíčovou roli, pokud jde o další formování digitální budoucnosti Evropy z průmyslového i obchodního hlediska, i co se týče každodenního života spotřebitelů používajících technologie nové generace. Vedle umělé inteligence, kvantové výpočetní techniky, vysoce výkonné výpočetní techniky, cloud computingu, technologií distribuované účetní knihy – zejména blockchainu – a veškerých dalších nových aplikací lze příležitosti pro udržitelný hospodářský růst a pro vysokou míru digitalizace naší společnosti dosáhnout pouze prostřednictvím kyberneticky bezpečných zařízení připojených k internetu.
3. KONSTATUJE, že v důsledku zvýšené míry používání spotřebitelských produktů a průmyslových zařízení připojených k internetu budou vzrůstat také nová rizika dotýkající se soukromí, bezpečnosti informací a kybernetické bezpečnosti, včetně množících se potenciálních důsledků pro integritu a dostupnost produktů a údajů, a to s přímým dopadem na bezpečnost. Tato rizika je nutno minimalizovat, a chránit tak spotřebitele, posílit celkovou kybernetickou odolnost Evropy a upevnit důvěru občanů v digitální řešení a technologie. Současně bude tímto způsobem posílena konkurenceschopnost a inovační schopnosti evropských poskytovatelů uvedených zařízení. Kybernetická bezpečnost a soukromí by měly být považovány za základní předpoklady procesů inovace, výroby a vývoje produktů včetně fáze návrhu (bezpečnost již od fáze návrhu) a měly by být zajištěny v průběhu celého životního cyklu daného produktu a v rámci celého souvisejícího dodavatelského řetězce.
4. ZDŮRAŽŇUJE, že stejně důležité jako zajištění vysoké úrovně bezpečnosti zařízení připojených k internetu je i prohlubování informovanosti spotřebitelů, pokud jde o možná rizika spojená s těmito zařízeními z hlediska soukromí a bezpečnosti. Snáze by tak bylo možno minimalizovat hrozby plynoucí z vysoké míry používání zařízení připojených k internetu, posilovat důvěru v jednotný digitální trh a maximálně využívat přínosů, které technologie těchto zařízení nabízejí na rovině hospodářské i společenské.

5. ZDŮRAZŇUJE, že účinnými pobídkami ke zvyšování bezpečnosti a zabezpečení zařízení připojených k internetu, a v důsledku pak i k posilování odolnosti inteligentních komunikačních sítí by mohly být veřejné investice do výzkumu a inovací, především prostřednictvím programů Horizont Evropa a Digitální Evropa, jakož i investice soukromé. Měly by také být urychleny investice do nezbytné digitální infrastruktury a technologií pro zavádění nejnovějších technologií zařízení připojených k internetu, má-li EU dosáhnout vedoucího postavení na průmyslové i digitální úrovni a má-li si zajistit strategickou autonomii, aniž by byla dotčena otevřená ekonomika.
6. ZDŮRAZŇUJE, že je třeba zajistit vysokou míru doplňkovosti a srovnatelnosti bezpečnostních funkcí systémů informačních a komunikačních technologií a jejich komponent, jež se používají v řadě různých odvětvích jednotného digitálního trhu.
7. BERE NA VĚDOMÍ činnost aktuálně probíhající na úrovni Unie, pokud jde o zvýšení úrovně kybernetické bezpečnosti zařízení připojených k internetu, zejména nedávné iniciativy Komise, jejichž cílem je řešit v krátkodobém horizontu aspekty kybernetické bezpečnosti v příslušných právních aktech, například v aktech obsažených v novém legislativním rámci, především směrnici 2014/53/EU (směrnice o rádiových zařízeních). ZDŮRAZŇUJE, že je důležité posoudit, do jaké míry je zapotřebí horizontální právní předpis, upřesňující rovněž nezbytné podmínky pro uvedení na trh, jenž by z dlouhodobého hlediska řešil všechny příslušné aspekty kybernetické bezpečnosti zařízení připojených k internetu, jako je dostupnost, integrita a důvěrnost. VÍTÁ v tomto ohledu diskusi, jejímž účelem je zvážit oblast působnosti takového právního předpisu a jeho propojení s rámcem pro certifikaci kybernetické bezpečnosti podle definice obsažené v aktu o kybernetické bezpečnosti, a to s cílem zvýšit bezpečnost v rámci jednotného digitálního trhu.
8. ZDŮRAZŇUJE, že aby se předešlo nejednoznačnosti a roztříštěnosti právní úpravy, požadavky na kybernetickou bezpečnost by měly být vymezeny v souladu s příslušnými právními předpisy Unie, včetně aktu o kybernetické bezpečnosti, nového legislativního rámce, nařízení o evropské harmonizaci a případného nového horizontálního právního předpisu.

9. UZNÁVÁ významnou úlohu všech zúčastněných stran, zejména výrobců, pokud jde o zvyšování úrovně kybernetické bezpečnosti zařízení připojených k internetu v rámci jednotného digitálního trhu, a VYBÍZÍ tudíž ke koordinaci a úzké spolupráci se všemi příslušnými zúčastněnými stranami z veřejného i soukromého sektoru, a to i se zřetelem k možnému novému horizontálnímu právnímu předpisu.
- 9a. VÍTÁ činnost probíhající pod vedením agentury ENISA, jejímž účelem je vypracovat návrhy prvních systémů EU pro certifikaci kybernetické bezpečnosti, konkrétně navrhovaných společných kritérií Evropské unie a navrhovaných systémů cloudových služeb. Tyto systémy budou pro certifikaci zařízení připojených k internetu významným východiskem.
10. ZDŮRAZŇUJE, že jakýkoli další systém certifikace pro zařízení připojená k internetu a související služby případně stanovený v průběžném pracovním programu Unie a definovaný v aktu o kybernetické bezpečnosti by měl určovat, jak mají být použitelné bezpečnostní požadavky plněny na příslušné úrovni záruky na základě konkrétních evropských a mezinárodně uznávaných norem – bez ohledu na odvětví, v němž má být produkt používán – a jaké mají být použity zkušební specifikace, certifikáty atd.
11. UZNÁVÁ, že certifikace zařízení připojených k internetu by vyžadovala příslušné standardy, normy nebo technické specifikace pro hodnocení kybernetické bezpečnosti podle aktu o kybernetické bezpečnosti. ZDŮRAZŇUJE tudíž, že je zapotřebí standardy, normy nebo technické specifikace kybernetické bezpečnosti pro zařízení připojená k internetu zavést a DOPORUČUJE evropským normalizačním organizacím, aby v této věci zintenzivnily úsilí. Zároveň BERE NA VĚDOMÍ normu ETSI 303 645 upravující kybernetickou bezpečnost spotřebitelských zařízení připojených k internetu věcí jakožto významný krok uvedeným směrem.

12. VYBÍZÍ Komisi, aby posoudila žádost o systémy certifikace kybernetické bezpečnosti pro zařízení připojená k internetu a související služby na základě v současnosti vypracovávaného průběžného pracovního programu Unie, s maximálním zřetelem k horizontálním evropským systémům certifikace kybernetické bezpečnosti, jejichž vývoj v současné době probíhá. Takový systém umožní výrobcům uvedených produktů, aby na dobrovolné bázi propagovali produkty s posouzenou úrovní záruky.
13. VYBÍZÍ k diskusi o způsobu, jak kybernetickou bezpečnost zakotvit jakožto cíl v budoucím horizontálním právní předpise, jenž se bude vztahovat na rizika v oblasti kybernetické bezpečnosti související se zařízeními připojenými k internetu, a současně KONSTATUJE, že je třeba zvážit, zda v příslušných případech není třeba přizpůsobit základní požadavky jednotlivých směrnic nového legislativního rámce.
14. VYZÝVÁ Komisi, aby v nezbytných případech rovněž posoudila doplňující odvětvová nařízení, jež by měla určovat, kterou úroveň kybernetické bezpečnosti by mělo dané zařízení připojené k internetu splňovat, aby bylo v případě zařízení obnášejících vyšší bezpečnostní rizika zajištěno uplatňování konkrétních požadavků na bezpečnost a soukromí.
15. ZDŮRAZŇUJE, že je třeba zvyšovat kvalitu života a blahobyt evropských občanů a posilovat důvěru v jednotný digitální trh. Bezpečnost a soukromí v rámci našich společností mají klíčový význam pro zachování našich základních hodnot, o něž se Unie opírá. ZDŮRAZŇUJE tudíž, že je třeba na základě rámce, jež poskytuje akt o kybernetické bezpečnosti, harmonizovat bezpečnostní požadavky v souladu s jednotlivými úrovněmi záruk napříč všemi odvětvími nového legislativního rámce, má-li být zabráněno roztříštěnosti a opakovaným kontrolám identických požadavků a mají-li být v celé Evropské unii zajištěny rovné podmínky pro hospodářskou soutěž a inovace.

16. VYZÝVÁ Komisi, Agenturu EU pro kybernetickou bezpečnost (ENISA), Výbor pro posuzování shody a pro dozor nad trhem v oblasti telekomunikací a Evropskou skupinu pro certifikaci kybernetické bezpečnosti (ECCG), aby se aktivně účastnily uvedené iniciativy, jíž má být posílen jednotný digitální trh a zvýšena důvěra v produkty, služby a procesy informačních technologií v souvislosti se zařízeními připojenými k internetu díky zajištění soukromí a kybernetické bezpečnosti, a aby zajistily maximální normy pro odolnost, bezpečnost a zabezpečení, a podpořily tak větší globální konkurenceschopnost průmyslu Unie činného v oblasti internetu věcí.
17. ZDŮRAZŇUJE v této souvislosti, že je zapotřebí podporovat malé a střední podniky jako základní stavební kámen evropského ekosystému kybernetické bezpečnosti, a VYBÍZÍ malé a střední podniky k účasti na všech již zahájených konzultacích, jakož i na normalizačních činnostech, jež tak budou moci zohledňovat jejich cenné a významné přispění k tomu, aby kybernetická bezpečnost představovala realistický cíl i konkurenční výhodu na evropském trhu.
18. KONSTATUJE, že povinnost zajistit kybernetickou bezpečnost a soukromí během celého životního cyklu konkrétního produktu a v rámci celého souvisejícího dodavatelského řetězce by mohla mít pozitivní dopad na environmentální stopu daného technologického odvětví, neboť výrobci by byli vedeni k používání inteligentních a udržitelných procesů vývoje a výroby, čímž by došlo ke snížení množství elektronického odpadu, jenž ve spojitosti s odstraňováním zařízení připojených k internetu vzniká.
-