

V Bruseli 2. decembra 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
ESPACE 77

VÝSLEDOK ROKOVANIA

Od:	Generálny sekretariát Rady
Dátum:	2. decembra 2020
Komu:	Delegácie

Predmet:	Závery Rady o kybernetickej bezpečnosti pripojených zariadení – závery Rady schválené písomným postupom
----------	--

Delegáciám zasielame v prílohe závery Rady o kybernetickej bezpečnosti pripojených zariadení, ktoré Rada schválila písomným postupom 2. decembra 2020.

Závery Rady o kybernetickej bezpečnosti pripojených zariadení

Rada Európskej únie,

PRIPOMÍNAJÚC:

- závery Rady o spoločnom oznámení Európskemu parlamentu a Rade: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ,
 - závery Rady o budovaní kapacít a spôsobilostí v oblasti kybernetickej bezpečnosti v EÚ,
 - závery Rady o význame 5G pre európske hospodárstvo a potrebe zmierniť bezpečnostné riziká spojené s 5G,
 - závery Rady o budúcnosti vysoko digitalizovanej Európy po roku 2020: „Zvýšenie digitálnej a hospodárskej konkurencieschopnosti v celej Únii a digitálna súdržnosť“,
 - závery Rady o formovaní digitálnej budúcnosti Európy,
 - závery Európskej rady o pandémie COVID-19, jednotnom trhu, priemyselnej politike, digitálnych a vonkajších vzťahoch,
 - oznámenie Európskej komisie o formovaní digitálnej budúcnosti Európy,
1. ZDÔRAZŇUJE, že Európska únia a jej členské štáty musia zabezpečiť svoju digitálnu zvrchovanosť a strategickú autonómiu a zároveň zachovať otvorené hospodárstvo. To zahŕňa posilnenie schopnosti prijímať autonómne technologické rozhodnutia a, ako jeden z hlavných pilierov, odolné a bezpečné infraštruktúry, produkty a služby na budovanie dôvery v digitálny jednotný trh a v rámci európskej spoločnosti. Základné hodnoty Európskej únie spočívajú najmä v zachovaní súkromia, bezpečnosti, rovnosti, ľudskej dôstojnosti, zásadách právneho štátu a otvorenom internete ako predpokladoch dosiahnutia spoločnosti, hospodárstva a priemyslu opierajúcich sa o digitálny rozvoj a zameraných na človeka.

2. PRIPOMÍNA rastúci význam pripojených zariadení a ich bezpečnosti vrátane strojových zariadení, snímačov a sietí, ktoré tvoria internet vecí. Pripojené zariadenia budú zohrávať kľúčovú úlohu pri ďalšom formovaní digitálnej budúcnosti Európy z priemyselného a podnikateľského hľadiska, ako aj v každodennom živote spotrebiteľov technológií novej generácie. Popri technológiách ako sú siete 5G, umelá inteligencia, kvantová výpočtová technika, vysokovýkonná výpočtová technika, cloud computing, technológie distribuovaných záznamov (predovšetkým blockchain) a ďalších nových aplikáciách možno príležitosti na udržateľný hospodársky rast a vyššiu úroveň digitalizácie našej spoločnosti dosahovať len prostredníctvom kyberneticky bezpečných pripojených zariadení.
3. POUKAZUJE NA TO, že zvýšené používanie spotrebných produktov a priemyselných zariadení pripojených na internet prinesie aj nové riziká pre súkromie, informácie a kybernetickú bezpečnosť vrátane čoraz väčšieho potenciálneho vplyvu na integritu a dostupnosť produktov a údajov, ktoré môžu priamo ovplyvňovať bezpečnosť. Je nevyhnutné minimalizovať takéto riziká s cieľom chrániť spotrebiteľov, posilniť celkovú kybernetickú odolnosť Európy a zvýšiť dôveru občanov v digitálne riešenia a technológie. Posilní sa tým aj konkurencieschopnosť a inovačné schopnosti európskych dodávateľov takýchto zariadení. Kybernetická bezpečnosť a ochrana súkromia by sa mali považovať za základné požiadavky pri inovácii produktov, výrobných a vývojových procesoch vrátane fázy navrhovania (bezpečnosť už v štádiu návrhu) a mali by byť zabezpečené počas celého životného cyklu produktu a v celom jeho dodávateľskom reťazci.
4. ZDÔRAZŇUJE, že okrem zabezpečenia vysokej úrovne bezpečnosti pripojených zariadení je rovnako dôležité zvýšiť informovanosť spotrebiteľov o potenciálnych rizikách pre ich súkromie a bezpečnosť. Pomohlo by to minimalizovať hrozby vyplývajúce zo zvýšeného používania pripojených zariadení, zvýšiť dôveru v digitálny jednotný trh a v maximálnej miere využívať hospodárske a spoločenské prínosy, ktoré ponúkajú technológie pripojených zariadení.

5. **PODČIARKUJE**, že verejné investície do výskumu a inovácie, najmä prostredníctvom programov Horizont Európa a Digitálna Európa, by spolu so súkromnými investíciami mohli vytvárať cenné stimuly na zvýšenie ochrany a bezpečnosti pripojených zariadení, a tým aj na zvýšenie odolnosti inteligentných komunikačných sietí. Mali by sa urýchliť aj investície do potrebnej digitálnej infraštruktúry a technológií na zavedenie najnovších technológií pripojených zariadení, aby sa dosiahlo vedúce postavenie priemyslu a digitálnych technológií a zabezpečila strategická autonómia, a to pri zachovaní otvorenej ekonomiky.
6. **ZDÔRAZŇUJE**, že je potrebné zabezpečiť vysokú úroveň komplementárnosti a porovnateľnosti bezpečnostných funkcií systémov IKT a zložiek IKT, ktoré sa používajú v mnohých odvetviach digitálneho jednotného trhu.
7. **BERIE NA VEDOMIE** súčasné vývojové trendy na úrovni Únie s cieľom zvýšiť úroveň kybernetickej bezpečnosti pripojených zariadení, najmä pokiaľ ide o nedávne iniciatívy Komisie zamerané na riešenie krátkodobých aspektov kybernetickej bezpečnosti IKT v príslušných právnych aktoch, napríklad v aktoch na základe nového legislatívneho rámca a osobitne v smernici 2014/53/EÚ (smernica o rádiových zariadeniach). **PODČIARKUJE**, že je z dlhodobého hľadiska dôležité posúdiť potrebu horizontálneho právneho predpisu, ktorý by tiež stanovoval potrebné podmienky prístupu na trh, s cieľom riešiť všetky relevantné aspekty kybernetickej bezpečnosti pripojených zariadení, ako je dostupnosť, integrita a dôvernosť. V tejto súvislosti **VÍTA** diskusiu o preskúmaní rozsahu pôsobnosti takéhoto právneho predpisu a jeho prepojenia s rámcom certifikácie kybernetickej bezpečnosti vymedzeným v akte o kybernetickej bezpečnosti s cieľom zvýšiť úroveň bezpečnosti na digitálnom jednotnom trhu.
8. **ZDÔRAZŇUJE**, že požiadavky na kybernetickú bezpečnosť by sa mali vymedziť v súlade s príslušnými právnymi predpismi Únie, okrem iného v akte o kybernetickej bezpečnosti, novom legislatívnom rámci, nariadení o európskej normalizácii a v možnom budúcom horizontálnom právnom predpise, aby sa predišlo nejasnostiam a fragmentácii v právnych predpisoch.

9. OCENŤUJE dôležitú úlohu všetkých zainteresovaných strán, najmä výrobcov, pri zvyšovaní úrovne kybernetickej bezpečnosti pripojených zariadení na digitálnom jednotnom trhu, a preto VYZÝVA na koordináciu a úzku spoluprácu so všetkými príslušnými verejnými a súkromnými zainteresovanými stranami, a to aj so zreteľom na možný budúci horizontálny právny predpis.
- 9a. VÍTA prebiehajúcu prácu pod vedením agentúry ENISA na vypracovaní prvých návrhov systémov certifikácie kybernetickej bezpečnosti EÚ, konkrétne navrhovaného systému spoločných kritérií Európskej únie a navrhovaného systému cloudových služieb. Tieto systémy vytvoria relevantné základy certifikácie pripojených zariadení.
10. ZDÔRAZŇUJE, že akýkoľvek dodatočný systém certifikácie pripojených zariadení a súvisiacich služieb, ktorý by bol ustanovený v priebežnom pracovnom programe Únie a vymedzený v akte o kybernetickej bezpečnosti, by mal určovať, ako by sa mali splniť uplatniteľné bezpečnostné požiadavky na príslušnom stupni dôveryhodnosti na základe osobitných európskych a medzinárodne uznávaných noriem bez ohľadu na odvetvie, v ktorom sa má daný produkt používať, a aké špecifikácie skúšok, certifikáty atď. sa majú uplatňovať.
11. PRIPÚŠŤA, že certifikácia pripojených zariadení by si vyžadovala príslušné normy, štandardy alebo technické špecifikácie pre hodnotenia kybernetickej bezpečnosti podľa aktu o kybernetickej bezpečnosti. Preto ZDÔRAZŇUJE potrebu stanoviť normy, štandardy alebo technické špecifikácie kybernetickej bezpečnosti pripojených zariadení a ODPORÚČA, aby sa posilnilo úsilie, ktoré v tejto veci vyvíjajú európske normalizačné organizácie. Zároveň BERIE NA VEDOMIE normu kybernetickej bezpečnosti ETSI EN 303 645 pre spotrebiteľské zariadenia internetu vecí ako dôležitý krok v tomto smere.

12. VYZÝVA Komisiu, aby zvážila žiadosť o [...] kandidátske systémy certifikácie kybernetickej bezpečnosti pripojených zariadení a súvisiace služby na základe priebežného pracovného programu Únie, ktorý sa v súčasnosti zostavuje, a aby popritom v maximálnej miere zohľadnila aktuálne vyvíjané horizontálne európske systémy certifikácie kybernetickej bezpečnosti. Takýto systém na dobrovoľnom základe umožní výrobcovi takýchto produktov propagovať produkty s posúdeným stupňom dôveryhodnosti.
13. VYZÝVA na diskusiu o tom, ako by sa cieľ kybernetickej bezpečnosti mohol zakotviť do budúceho horizontálneho právneho predpisu, ktorý sa bude vzťahovať na kyberneticko-bezpečnostné riziká súvisiace s pripojenými zariadeniami, a zároveň POUKAZUJE na potrebu zvážiť prípadné prispôsobenie základných požiadaviek príslušných smerníc nového legislatívneho rámca.
14. NABÁDA Komisiu, aby v prípade potreby posúdila aj doplnkové odvetvové predpisy, v ktorých by sa malo vymedzovať, akú úroveň kybernetickej bezpečnosti by mali pripojené zariadenia dosahovať, aby sa zabezpečilo zavedenie osobitných požiadaviek na bezpečnosť a ochranu súkromia pre takéto zariadenia s vyššími bezpečnostnými rizikami.
15. ZDÔRAZŇUJE potrebu zlepšiť kvalitu života a životných podmienok európskych občanov a posilniť dôveru v digitálny jednotný trh. Bezpečnosť a súkromie majú v našich spoločnostiach kľúčový význam pre zachovanie našich základných úijných hodnôt. Preto ZDÔRAZŇUJE, že bude potrebné vychádzať z rámca, ktorý poskytuje akt o kybernetickej bezpečnosti, s cieľom harmonizovať bezpečnostné požiadavky podľa rôznych stupňov dôveryhodnosti vo všetkých odvetviach nového legislatívneho rámca, aby sa zabránilo fragmentácii a viacnásobným kontrolám rovnakých požiadaviek a aby sa v celej Európskej únii vytvorili rovnaké podmienky na hospodársku súťaž a inováciu.

16. VYZÝVA Komisiu, Agentúru EÚ pre kybernetickú bezpečnosť (ENISA), Výbor pre posudzovanie zhody a pre dozor nad trhom v oblasti telekomunikácií a Európsku skupinu pre certifikáciu kybernetickej bezpečnosti, aby sa aktívne zapájali do tejto iniciatívy na posilnenie digitálneho jednotného trhu a zvýšenie dôvery v produkty, služby a procesy IKT pre pripojené zariadenia zabezpečením súkromia a kybernetickej bezpečnosti, a aby uľahčovali zvýšenú globálnu konkurencieschopnosť odvetvia internetu vecí Únie prostredníctvom zaistenia najvyšších noriem odolnosti, ochrany a bezpečnosti.
17. V tejto súvislosti ZDÔRAZŇUJE potrebu podporovať MSP ako základný stavebný prvok európskeho ekosystému kybernetickej bezpečnosti a NABÁDA MSP, aby sa zúčastňovali na všetkých otváraných verejných konzultáciách, ako aj na normalizačných činnostiach, aby sa tak zohľadnil ich cenný a významný prínos k tomu, aby sa kybernetická bezpečnosť stala dosiahnuteľným cieľom a aj konkurenčnou výhodou na európskom trhu.
18. POZNAMENÁVA, že povinnosť zabezpečiť kybernetickú bezpečnosť a súkromie počas celého životného cyklu produktu a v celom jeho dodávateľskom reťazci by mohla mať pozitívny vplyv na environmentálnu stopu technologického odvetvia tým, že by viedla výrobcov k inteligentnému a udržateľnému vývoju a výrobným procesom, čím by sa znížilo množstvo elektronického odpadu pri zneškodňovaní pripojených zariadení.
-