

Bruselj, 2. december 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

IZID POSVETOVANJA

Pošiljatelj: generalni sekretariat Sveta

Datum: 2. december 2020

Prejemnik: delegacije

Zadeva: Sklepi Sveta o kibernetiki varnosti povezanih naprav
– sklepi Sveta, odobreni po pisnem postopku

V prilogi vam pošiljamo sklepe Sveta o kibernetiki varnosti povezanih naprav, ki jih je Svet odobril 2. decembra 2020 po pisnem postopku.

Sklepi Sveta o kibernetiski varnosti povezanih naprav

Svet Evropske unije –

OB SKLICEVANJU NA:

- sklepe Sveta o Skupnem sporočilu Evropskemu parlamentu in Svetu z naslovom „Odpornost, odvratanje in obramba: okrepitev kibernetiske varnosti za EU“,
 - sklepe Sveta o krepitvi zmogljivosti in zmožnosti na področju kibernetiske varnosti v EU,
 - sklepe Sveta o pomenu omrežij 5G za evropsko gospodarstvo in dejstvu, da je treba zmanjšati varnostna tveganja, povezana z njimi,
 - sklepe Sveta o prihodnosti visoko digitalizirane Evrope po letu 2020 z naslovom „Krepitev digitalne in gospodarske konkurenčnosti v Uniji ter digitalna kohezija“,
 - sklepe Sveta o oblikovanju digitalne prihodnosti Evrope,
 - sklepe Evropskega sveta o covidu-19, enotnem trgu, industrijski politiki, digitalni razsežnosti in zunanjih odnosih,
 - sporočilo Evropske komisije o oblikovanju digitalne prihodnosti Evrope –
1. POUDARJA, da morajo Evropska unija in njene države članice poskrbeti, da bodo digitalno suverene in strateško avtonomne, hkrati pa ohranile odprto gospodarstvo. To vključuje krepitev sposobnosti sprejemanja avtonomnih tehnoloških odločitev ter – kot enega od glavnih stebrov – izgradnje odporne in varne infrastrukture, izdelkov in storitev za vzpostavitev zaupanja v enotni digitalni trg v evropski družbi. Temeljne vrednote Evropske unije so usmerjene zlasti v ohranjanje zasebnosti, varnosti, enakosti, človekovega dostojanstva, pravne države in odprtega interneta kot predpogojev za doseganje na človeka osredotočene družbe, gospodarstva in industrije, katerih gonilo je digitalizacija;

2. PRIZNAVA vse večji pomen povezanih naprav in njihove varnosti, vključno s stroji, senzorji in omrežji, ki tvorijo internet stvari (IoT). Povezane naprave bodo imele ključno vlogo pri nadaljnjem oblikovanju digitalne prihodnosti Evrope, tako z industrijskega in poslovnega vidika kot v vsakdanjem življenju potrošnikov nove generacije tehnologij. Poleg 5G je mogoče umetno inteligenco, kvantno računalništvo, visokozmogljivostno računalništvo, računalništvo v oblaku, tehnologije razpršene evidence, kot je blokovna veriga, ter kakršne koli druge nove aplikacije in priložnosti za trajnostno gospodarsko rast in višjo stopnjo digitalizacije naše družbe doseči le s pomočjo kibernetско varnih povezanih naprav;
3. UGOTAVLJA, da bodo s pogostejšo uporabo potrošniških izdelkov in industrijskih naprav, povezanih z internetom, večja tudi nova tveganja za zasebnost ter informacijsko in kibernetско varnost, vključno z vse večjimi možnimi učinki na celovitost in razpoložljivost izdelkov in podatkov, kar lahko vpliva neposredno na varnost. Ključnega pomena je, da se ta tveganja kar se da zmanjšajo, da bi tako zaščitili potrošnike, okrepili splošno kibernetско odpornost Evrope ter poglobili zaupanje državljanov v digitalne rešitve in tehnologije. To bo hkrati spodbudilo konkurenčnost in inovacijske zmogljivosti evropskih ponudnikov takih naprav. Kibernetско varnost in zasebnost bi bilo treba priznati kot bistveni zahtevi pri izdelčnih inovacijah ter proizvodnih in razvojnih procesih, vključno s fazo zasnove (vgrajena varnost), hkrati pa ju zagotavljati v celotnem življenjskem ciklu izdelka in v njegovi celotni dobavni verigi;
4. NAGLAŠA, da je poleg zagotavljanja visoke ravni varnosti povezanih naprav pomembna tudi boljša obveščenost potrošnikov o morebitnih tveganjih v zvezi z zasebnostjo in varnostjo. To bi pripomoglo k zmanjšanju groženj, ki izhajajo iz pogostejše uporabe povezanih naprav, k poglobitvi zaupanja v enotni digitalni trg ter h kar največjemu izkoristku gospodarskih in družbenih koristi, ki jih prinašajo tehnologije povezanih naprav;

5. POUDARJA, da bi lahko javne naložbe v raziskave in inovacije, zlasti prek programa Obzorje Evropa in programa za digitalno Evropo, skupaj z zasebnimi naložbami ustvarile dragocene spodbude za izboljšanje varnosti in zaščite povezanih naprav ter povečanje odpornosti pametnih komunikacijskih omrežij. Pospešiti bi bilo treba tudi naložbe v potrebno digitalno infrastrukturo in tehnologijo za uvedbo najnovejših tehnologij povezanih naprav, s čimer bi dosegli vodilni položaj v industriji in na digitalnem področju ter zagotovili strateško avtonomijo, hkrati pa ohranili odprto gospodarstvo;
6. IZPOSTAVLJA potrebo po zagotovitvi visoke ravni dopolnjevanja in primerljivosti varnostnih funkcionalnosti sistemov IKT in komponent IKT, ki se uporabljajo v najrazličnejših sektorjih enotnega digitalnega trga;
7. SE SEZNANJA s trenutnim razvojem dogodkov na ravni Unije v zvezi z dvigom ravni kibernetске varnosti povezanih naprav, zlasti glede nedavnih pobud Komisije za kratkoročno obravnavo vidikov kibernetске varnosti v ustreznih pravnih aktih, denimo v aktih iz novega zakonodajnega okvira, zlasti Direktivi 2014/53/EU (direktiva o radijski opremi); POUDARJA, da je treba oceniti, ali je dolgoročno potrebna horizontalna zakonodaja, v kateri bi med drugim določili potrebne pogoje za dajanje na trg in obravnavali vse ustrezne vidike kibernetске varnosti povezanih naprav, kot so razpoložljivost, celovitost in zaupnost; v zvezi s tem POZDRAVLJA razpravo, v okviru katere bi preučili področje uporabe take zakonodaje in njene povezave s certifikacijskim okvirom za kibernetsko varnost, kot je opredeljen v aktu o kibernetски varnosti, da bi se dvignila raven varnosti znotraj enotnega digitalnega trga;
8. POUDARJA, da bi bilo treba zahteve glede kibernetске varnosti opredeliti v skladu z ustrežno zakonodajo Unije, tudi certifikacijskim okvirom za kibernetsko varnost, novim zakonodajnim okvirom, uredbo o evropski standardizaciji in morebitno prihodnjo horizontalno zakonodajo, s čimer bi se izognili dvomnosti in razdrobljenosti zakonodaje;

9. PREPOZNAVA pomembno vlogo vseh deležnikov, zlasti proizvajalcev, pri dvigu ravni kibernetske varnosti povezanih naprav na enotnem digitalnem trgu, zato POZIVA k usklajevanju in tesnemu sodelovanju z vsemi ustreznimi javnimi in zasebnimi deležniki, tudi v luči morebitne prihodnje horizontalne zakonodaje;
- 9a. POZDRAVLJA potekajoča prizadevanja agencije ENISA, da pripravi osnutek prvih certifikacijskih shem EU za kibernetsko varnost, in sicer predlaganih skupnih meril Evropske unije in predlaganih shem storitev v oblaku. Te sheme bodo pomembna osnova za certificiranje povezanih naprav;
10. NAGLAŠA, da bi morale biti v vsaki dodatni certifikacijski shemi za povezane naprave in z njimi povezane storitve, ki bi bila določena v tekočem delovnem programu Unije in opredeljena v certifikacijskem okviru za kibernetsko varnost, določeno, kako bi bilo treba izpolniti veljavne varnostne zahteve na ustrezni ravni zanesljivosti na podlagi posebnih evropskih in mednarodno priznanih standardov, ne glede na sektor, v katerem naj bi se izdelek uporabljal, ter katere preskusne specifikacije, certifikati itn. naj bi se uporabljali;
11. PRIZNAVA, da bi certificiranje povezanih naprav zahtevalo ustrezne norme, standarde ali tehnične specifikacije za ocenjevanje kibernetske varnosti v certifikacijskem okviru za kibernetsko varnost; zato IZPOSTAVLJA potrebo po določitvi norm, standardov oziroma tehničnih specifikacij za kibernetsko varnost povezanih naprav ter PRIPOROČA okrepitev tozadevnih prizadevanj evropskih organizacij za standardizacijo; hkrati UGOTAVLJA, da je standard ETSI EN 303 645 za kibernetsko varnost potrošniških naprav interneta stvari pomemben korak v tej smeri;

12. POZIVA Komisijo, naj preuči zahtevo za kandidate za certifikacijske sheme za kibernetško varnost povezanih naprav in z njimi povezanih storitev na podlagi tekočega delovnega programa Unije, ki je v pripravi, pri tem pa v največji možni meri upošteva horizontalne evropske certifikacijske sheme za kibernetško varnost, ki so v pripravi. S to shemo, ki bo prostovoljna, bodo lahko proizvajalci takih izdelkov slednje promovirali z ocenjeno ravno zanesljivosti;
13. POZIVA k razpravi o tem, kako bi lahko cilj kibernetške varnosti vključili v prihodnjo horizontalno zakonodajo, ki zajema tveganja za kibernetško varnost v zvezi s povezanimi napravami, hkrati pa UGOTAVLJA, da je treba po potrebi razmisliti o prilagoditvi bistvenih zahtev iz zadevnih direktiv iz novega zakonodajnega okvira;
14. SPODBUJA Komisijo, naj po potrebi oceni tudi dopolnilne predpise za posamezen sektor, v katerih bi moralo biti opredeljeno, katero raven kibernetške varnosti bi morala izpolnjevati povezana naprava, s čimer bi zagotovili, da se za take naprave z večjimi varnostnimi tveganji določijo posebne zahteve glede varnosti in zasebnosti;
15. POUDARJA, da je treba izboljšati kakovost življenja in blaginjo evropskih državljanov in državljanek ter okrepiti zaupanje v enotni digitalni trg. Varnost in zasebnost naših družb sta bistvenega pomena za ohranjanje naših temeljnih vrednot Unije. Zato POUDARJA tudi, da je treba nadgraditi okvir, ki ga zagotavlja certifikacijski okvir za kibernetško varnost, za uskladitev varnostnih zahtev glede na različne ravni zanesljivosti v vseh sektorjih novega zakonodajnega okvira, da bi se izognili razdrobljenosti in večkratnim preverjanjem enakih zahtev ter v vsej Evropski uniji zagotovili enake konkurenčne pogoje za konkurenco in inovacije;

16. POZIVA Komisijo, Agencijo EU za kibernetско varnost (ENISA), Odbor za ugotavljanje skladnosti in nadzorovanje telekomunikacijskega trga (TCAM) ter Evropsko certifikacijsko skupino za kibernetско varnost (ECCG), naj z zagotavljanjem zasebnosti in kibernetске varnosti dejavno sodelujejo pri tej pobudi za krepitev enotnega digitalnega trga ter poglobitev zaupanja v izdelke, storitve in procese IKT za povezane naprave, hkrati pa z zagotavljanjem najvišjih standardov odpornosti, varnosti in zaščite spodbujajo večjo svetovno konkurenčnost industrije Unije na področju interneta stvari;
17. v zvezi s tem IZPOSTAVLJA, da je treba podpirati MSP kot bistvene gradnike evropskega ekosistema kibernetске varnosti, MSP pa SPODBUJA, naj sodelujejo v vseh organiziranih javnih posvetovanjih in dejavnostih standardizacije ter tako koristno in pomembno prispevajo, da bo kibernetска varnost postala dosegljiv cilj in konkurenčna prednost na evropskem trgu;
18. UGOTAVLJA, da bi obveznost zagotavljanja kibernetске varnosti in zasebnosti v celotnem življenjskem ciklu izdelka in v njegovi celotni dobavni verigi lahko pozitivno vplivala na okoljski odtis tehnološkega sektorja, saj bi proizvajalce vodila k pametnemu in trajnostnemu razvoju in proizvodnim procesom ter s tem zmanjšala količino elektronskih odpadkov, povezanih z odstranjevanjem povezanih naprav.
