Eiropas Savienības
Padome

Briselē, 2020. gada 2. decembrī
(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

DARBA REZULTĀTI

Sūtītājs:	Padomes Ģenerālsekretariāts
Datums:	2020. gada 2. decembris
Saņēmējs:	delegācijas
Temats:	Padomes secinājumi par savienoto ierīču kiberdrošību - Padomes secinājumi, kas apstiprināti, izmantojot rakstisko procedūru

Pielikumā ir pievienoti Padomes secinājumi par savienoto ierīču kiberdrošību, kurus Padome, izmantojot rakstisko procedūru, apstiprināja 2020. gada 2. decembrī.

PIELIKUMS

Padomes secinājumi par savienoto ierīču kiberdrošību

Eiropas Savienības Padome,

ATGĀDINOT

- Padomes secinājumus par kopīgo paziņojumu Eiropas Parlamentam un Padomei "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību",
- Padomes secinājumus par kiberdrošības spēju un spēju veidošanu ES,
- Padomes secinājumus par 5G nozīmi Eiropas ekonomikā un nepieciešamību mazināt ar 5G saistītos drošības riskus,
- Padomes secinājumus par augsti digitalizētas Eiropas nākotni pēc 2020. gada: "Visas Savienības digitālās un ekonomiskās konkurētspējas un digitālās kohēzijas stiprināšana",
- Padomes secinājumus par Eiropas digitālās nākotnes veidošanu,
- Eiropadomes secinājumus par Covid-19, vienoto tirgu, rūpniecības politiku, digitālo dimensiju un ārējām attiecībām,
- Eiropas Komisijas paziņojumu par Eiropas digitālās nākotnes veidošanu.

1. UZSVER, ka Eiropas Savienībai un tās dalībvalstīm ir jānodrošina sava digitālā suverenitāte un stratēģiskā autonomija, vienlaikus saglabājot atvērtu ekonomiku. Tas nozīmē arī stiprināt spēju izdarīt autonomas tehnoloģiskas izvēles un – kā vienu no galvenajiem pīlāriem – noturīgas un drošas infrastruktūras, produktus un pakalpojumus, ar mērķi veidot uzticēšanos digitālajam vienotajam tirgum, Eiropas sabiedrībā. Eiropas Savienības pamatvērtības jo īpaši aizsargā privātumu, drošību, līdztiesību, cilvēka cieņu, tiesiskumu un atvērtu internetu kā priekšnoteikumus, lai izveidotu digitāli orientētu, uz cilvēku vērstu sabiedrību, ekonomiku un rūpniecību.

2. ATZĪST, ka savienotās ierīces un to drošība, tostarp iekārtas, sensori un tīkli, kas veido lietu internetu, kļūst arvien svarīgākas. Savienotajām ierīcēm būs svarīga loma Eiropas digitālās nākotnes turpmākā veidošanā no rūpniecības un uzņēmējdarbības viedokļa, kā arī jaunās paaudzes tehnoloģiju patērētāju ikdienas dzīvē. Papildus 5G, mākslīgo intelektu, kvantisko datošanu, augstas veiktspējas datošanu, mākoņdatošanu, sadalītās virsgrāmatas tehnoloģijas, proti, blokķēdi, un jebkādas citas jaunas lietojumprogrammatūras un iespējas ilgtspējīgai ekonomikas izaugsmei un augstākam mūsu sabiedrības digitalizācijas līmenim var īstenot tikai ar kiberdrošām savienotajām ierīcēm.

3. ATZĪMĒ, ka plašāka tādu patēriņa preču un rūpniecisko ierīču izmantošana, kas savienotas ar internetu, arī radīs jaunus riskus privātumam, informācijas drošībai un kiberdrošībai, tostarp arvien lielāku iespējamo ietekmi uz produktu un datu integritāti un pieejamību, un tas var tieši ietekmēt drošumu. Ir būtiski maksimāli samazināt šādus riskus, lai aizsargātu patērētājus, stiprinātu Eiropas vispārējo kibernoturību un palielinātu iedzīvotāju uzticēšanos digitālajiem risinājumiem un tehnoloģijām. Tas arī sekmēs šādu ierīču nodrošinātāju Eiropā konkurētspēju un inovācijas spējas. Kiberdrošība un privātums būtu jāatzīst par pamatprasībām produktu inovācijas, ražošanas un izstrādes procesos, tostarp projektēšanas posmā (integrētā drošība), un tie būtu jānodrošina visā produkta aprites ciklā un visā tā piegādes ķēdē.

4. UZSVER, ka papildus tam, ka tiek nodrošināts augsts savienoto ierīču drošības līmenis, vienlīdz svarīgi ir palielināt patērētāju informētību par iespējamiem riskiem viņu privātumam un drošībai. Tas palīdzētu līdz minimumam samazināt apdraudējumus, ko rada savienoto ierīču plašāka izmantošana, vairotu uzticēšanos digitālajam vienotajam tirgum un palīdzētu maksimāli izmantot ekonomiskos un sabiedriskos ieguvumus, ko sniedz savienoto ierīču tehnoloģijas.

5. UZSVER, ka publiskās investīcijas pētniecībā un inovācijā, jo īpaši ar programmām "Apvārsnis Eiropa" un "Digitālā Eiropa", kā arī privātās investīcijas varētu radīt vērtīgus stimulus, lai savienotās ierīces padarītu drošākas un aizsargātākas un tādējādi viedos sakaru tīklus – noturīgākus. Lai kļūtu par līderi rūpniecības un digitālajā jomā un nodrošinātu stratēģisko autonomiju, vienlaikus saglabājot atvērtu ekonomiku, būtu arī jāpaātrina investīcijas digitālajā infrastruktūrā un tehnoloģijā, kas vajadzīga, lai izvērstu jaunākās savienoto ierīču tehnoloģijas.

6. UZSVER, ka ir jānodrošina augsts to IKT sistēmu un IKT komponentu drošības funkciju papildināmības un salīdzināmības līmenis, kurus izmanto daudzās dažādās digitālā vienotā tirgus nozarēs.

7. ATZINĪGI VĒRTĒ pašreizējās norises Savienības līmenī, kuru mērķis ir paaugstināt savienoto ierīču kiberdrošības līmeni, jo īpaši attiecībā uz Komisijas nesenajām iniciatīvām īsā termiņā pievērsties kiberdrošības aspektiem attiecīgajos tiesību aktos, piemēram, aktos saskaņā ar jauno tiesisko regulējumu (JTR), jo īpaši Direktīvā 2014/53/ES (Radioiekārtu direktīva). UZSVER, ka ir svarīgi izvērtēt vajadzību pēc horizontāla tiesību akta, arī precizējot nepieciešamos nosacījumus attiecībā uz laišanu tirgū, ilgtermiņā, lai pievērstos visiem attiecīgajiem savienoto ierīču kiberdrošības aspektiem, piemēram, pieejamībai, integritātei un konfidencialitātei. Šajā sakarā ATZINĪGI VĒRTĒ diskusiju, kuras mērķis ir izpētīt šāda tiesību akta darbības jomu un tā saiknes ar kiberdrošības sertifikācijas satvaru, kā noteikts Kiberdrošības aktā (KDA), ar mērķi paaugstināt drošības līmeni digitālajā vienotajā tirgū.

8. UZSVER – lai izvairītos no neskaidrības un tiesību aktu sadrumstalotības, kiberdrošības prasības būtu jādefinē saskaņā ar attiecīgajiem Savienības tiesību aktiem, tostarp KDA, JTR, Regulu par Eiropas standartizāciju un iespējamo turpmāko horizontālo tiesību aktu.

9. ATZĪST svarīgo lomu, kāda ir visām ieinteresētajām personām, jo īpaši ražotājiem, lai paaugstinātu savienoto ierīču kiberdrošības līmeni digitālajā vienotajā tirgū, tādēļ AICINA nodrošināt koordināciju un ciešu sadarbību ar visām attiecīgajām publiskajām un privātajām ieinteresētajām personām, arī ņemot vērā iespējamu turpmāku horizontālo tiesību aktu.

9.a ATZINĪGI VĒRTĒ pašreizējo darbu *ENISA* vadībā pie tā, lai izstrādātu projektu pirmajām ES kiberdrošības sertifikācijas shēmām, proti, ierosinātos Eiropas Savienības kopējos kritērijus un ierosinātās mākoņpakalpojumu shēmas. Šīs shēmas būs relevants pamats savienoto ierīču sertificēšanai.

10. UZSVER, ka jebkādās savienoto ierīču un saistīto pakalpojumu papildu sertifikācijas shēmās, kas būtu paredzētas Savienības mainīgajā darba programmā un definētas saskaņā ar KDA, būtu jāprecizē, kā būtu jāievēro piemērojamās drošības prasības attiecīgajā apliecinājuma līmenī, pamatojoties uz konkrētiem Eiropas un starptautiski atzītiem standartiem, neatkarīgi no nozares, kurā produktu paredzēts izmantot, un kādas testu specifikācijas, sertifikāti utt. ir jāpiemēro.

11. ATZĪST, ka savienoto ierīču sertifikācijai būtu nepieciešamas attiecīgas normas, standarti vai tehniskās specifikācijas kiberdrošības izvērtējumiem saskaņā ar KDA. Tāpēc UZSVER, ka ir jānosaka kiberdrošības normas, standarti vai tehniskās specifikācijas savienotajām ierīcēm, un IESAKA pastiprināt Eiropas standartizācijas organizāciju centienus šajā jomā. Vienlaikus ATZĪMĒ ETSI EN 303 645 kiberdrošības standartu patērētāju lietu interneta ierīcēm kā svarīgu soli šajā virzienā.

12. AICINA Komisiju apsvērt prasību attiecībā uz [...] kiberdrošības sertifikācijas kandidātshēmām savienotajām ierīcēm un saistītajiem pakalpojumiem, pamatojoties uz Savienības mainīgo darba programmu, kas patlaban tiek izstrādāta, maksimāli ņemot vērā Eiropas kiberdrošības horizontālās sertifikācijas shēmas, kas patlaban tiek izstrādātas. Šāda shēma pēc brīvprātības principa ļaus šādu produktu ražotājiem reklamēt produktus ar novērtēto apliecinājuma līmeni.

13. AICINA rīkot diskusiju par to, kā kiberdrošības mērķi varētu nostiprināt turpmākā horizontālajā tiesību aktā, kurš ietvers kiberdrošības riskus saistībā ar savienotajām ierīcēm, un vienlaikus ATZĪMĒ, ka attiecīgā gadījumā ir jāapsver attiecīgo JTR direktīvu būtisko prasību pielāgošana.

14. MUDINA Komisiju vajadzības gadījumā arī novērtēt papildu noteikumus konkrētās nozarēs, kuros būtu jānosaka, kāds kiberdrošības līmenis savienotajai ierīcei būtu jāsasniedz, lai nodrošinātu, ka attiecībā uz šādām ierīcēm ar augstākiem drošības riskiem ir ieviestas īpašas drošības un privātuma prasības.

15. UZSVER, ka ir jāuzlabo Eiropas iedzīvotāju dzīves kvalitāte un labklājība un jāveicina uzticēšanās digitālajam vienotajam tirgum. Mūsu sabiedrības drošība un privātums ir būtiski, lai aizsargātu Savienības pamatvērtības. Tādēļ UZSVER, ka ir jābalstās uz KDA sniegto satvaru, lai saskaņotu drošības prasības atbilstoši dažādiem apliecinājuma līmeņiem visās JTR nozarēs nolūkā izvairīties no sadrumstalotības un vienādu prasību vairākkārtējām pārbaudēm un visā Eiropas Savienībā nodrošinātu vienlīdzīgus konkurences un inovācijas apstākļus.

16. AICINA Komisiju, ES Kiberdrošības aģentūru (*ENISA*), Telekomunikāciju atbilstības novērtēšanas un tirgus uzraudzības komiteju un Eiropas Kiberdrošības sertifikācijas grupu (*ECCG*) aktīvi piedalīties šajā iniciatīvā par digitālā vienotā tirgus stiprināšanu un uzticības palielināšanu IKT produktiem, pakalpojumiem un procesiem savienotajām ierīcēm, nodrošinot privātumu un kiberdrošību, un veicināt lielāku Savienības lietu interneta nozares globālo konkurētspēju, nodrošinot visaugstākos noturības, drošuma un drošības standartus.

17. Šajā sakarā UZSVER, ka ir jāatbalsta mazie un vidējie uzņēmumi (MVU), kas ir būtisks Eiropas kiberdrošības ekosistēmas elements, un MUDINA MVU piedalīties visās sāktajās sabiedriskajās apspriešanās, kā arī standartizācijas darbībās, kā mērķis ir ņemt vērā to vērtīgo un nozīmīgo ieguldījumu ceļā uz to, lai padarītu kiberdrošību par sasniedzamu mērķi, kā arī konkurences priekšrocību Eiropas tirgū.

18. ATZĪMĒ, ka pienākumam nodrošināt kiberdrošību un privātumu visā produkta aprites ciklā un visā tā piegādes ķēdē varētu būt pozitīva ietekme uz tehnoloģiju nozares vides pēdas nospiedumu, vadošiem ražotājiem virzoties uz viediem un ilgtspējīgiem izstrādes un ražošanas procesiem un tādējādi samazinot to elektronisko atkritumu apjomu, kas saistīti ar savienoto ierīču iznīcināšanu.