

Bruxelles, 2. prosinca 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

ISHOD POSTUPAKA

Od:	Glavno tajništvo Vijeća
Na datum:	2. prosinca 2020.
Za:	Delegacije
Predmet:	Zaključci Vijeća o kibersigurnosti povezanih uređaja – zaključci Vijeća odobreni pisanim postupkom

Za delegacije se u prilogu nalaze Zaključci Vijeća o kibersigurnosti povezanih uređaja koje je Vijeće odobrilo pisanim postupkom 2. prosinca 2020.

Zaključci Vijeća o kibersigurnosti povezanih uređaja

Vijeće Europske unije,

PODSJEĆAJUĆI NA

- zaključke Vijeća o Zajedničkoj komunikaciji Europskom parlamentu i Vijeću: Otpornost, odvratanje i obrana: jačanje kibersigurnosti EU-a,
 - zaključke Vijeća o izgradnji kapaciteta i sposobnosti u području kibersigurnosti u EU-u,
 - zaključke Vijeća o važnosti mreža 5G za europsko gospodarstvo i potrebi za ublažavanjem sigurnosnih rizika povezanih s mrežama 5G,
 - zaključke Vijeća o budućnosti visoko digitalizirane Europe nakon 2020.: „Poticanje digitalne i gospodarske konkurentnosti u cijeloj Uniji i digitalna kohezija”,
 - zaključke Vijeća o oblikovanju digitalne budućnosti Europe,
 - zaključke Europskog vijeća o bolesti COVID-19, jedinstvenom tržištu, industrijskoj politici, digitalnim pitanjima i vanjskim odnosima,
 - komunikaciju Europske komisije pod naslovom „Oblikovanje digitalne budućnosti Europe”;
1. ISTIČE da Europska unija i njezine države članice trebaju osigurati svoju digitalnu suverenost i stratešku autonomiju, uz očuvanje otvorenog gospodarstva. To uključuje jačanje sposobnosti donošenja autonomnih tehnoloških odabira i, kao jedan od glavnih stupova, otporne i sigurne infrastrukture, proizvode i usluge za izgradnju povjerenja u jedinstveno digitalno tržište i unutar europskog društva. Temeljne vrijednosti Europske unije osobito služe očuvanju privatnosti, sigurnosti, jednakosti, ljudskog dostojanstva, vladavine prave i otvorenog interneta kao preduvjetâ za ostvarenje društva, gospodarstva i industrije koji se temelje na digitalizaciji, a usmjereni su na čovjeka.

2. **PREPOZNAJE** sve veću važnost povezanih uređaja i njihove sigurnosti, uključujući strojeve, senzore i mreže koje čine internet stvari. Povezani uređaji imaju ključnu ulogu u daljnjem oblikovanju digitalne budućnosti Europe, s industrijskog i poslovnog gledišta, kao i u svakodnevnom životu potrošača nove generacije tehnologije. Kao i 5G tehnologija, umjetna inteligencija, kvantno računalstvo, računalstvo visokih performansi, računalstvo u oblaku, tehnologije decentraliziranog vođenja evidencije transakcija odnosno lanac blokova i sve druge nove aplikacije i prilike za održiv gospodarski rast i višu razinu digitalizacije našeg društva mogu se postići samo s pomoću kibersigurnih povezanih uređaja.
3. **NAPOMINJE** da će povećana upotreba potrošačkih proizvoda i industrijskih uređaja povezanih na internet ujedno dovesti do novih rizika u pogledu privatnosti, informacijske sigurnosti i kibersigurnosti, uključujući sve veće potencijalne učinke na cjelovitost i dostupnost proizvoda i podataka, što može izravno utjecati na sigurnost. Ključno je takve rizike svesti na najmanju moguću mjeru kako bi se zaštitili potrošači, ojačala opća kiberotpornost Europe i povećalo povjerenje građana u digitalna rješenja i tehnologije. Time će se ujedno potaknuti konkurentnost i inovacijske sposobnosti europskih pružatelja takvih uređaja. Kibersigurnost i privatnost trebalo bi priznati kao ključne zahtjeve u postupcima inovacija, proizvodnje i razvoja proizvoda, uključujući fazu projektiranja (integrirana sigurnost), te bi ih trebalo osigurati tijekom cijelog životnog ciklusa proizvoda i duž cijelog opskrbnog lanca.
4. **NAGLAŠAVA** da je, uz osiguravanje visoke razine sigurnosti povezanih uređaja, jednako važno povećati osviještenost potrošača o njihovim potencijalnim rizicima u pogledu privatnosti i sigurnosti. Time bi se pomoglo u minimiziranju prijetnji nastalih uslijed povećane upotrebe povezanih uređaja, poboljšanju povjerenja u jedinstveno digitalno tržište i optimalnom iskorištavanju ekonomskih i socijalnih prednosti koje nude tehnologije povezanih uređaja.

5. ISTIČE da bi se javnim ulaganjima u istraživanje i inovacije, posebno u okviru programâ Obzor Europa i Digitalna Europa, kao i privatnim ulaganjima, mogli stvoriti vrijedni poticaji s ciljem postizanja veće zaštite i sigurnosti povezanih uređaja, a time i veće otpornosti pametnih komunikacijskih mreža. Trebalo bi ubrzati i ulaganja u potrebnu digitalnu infrastrukturu i tehnologiju za uvođenje najnovijih tehnologija povezanih uređaja kako bi se postiglo industrijsko i digitalno vodstvo te osigurala strateška autonomija, uz očuvanje otvorenoga gospodarstva.
6. ISTIČE potrebu za osiguravanjem visoke razine komplementarnosti i usporedivosti sigurnosnih funkcionalnosti sustavâ IKT-a i komponenti IKT-a, koji se upotrebljavaju u nizu različitih sektora jedinstvenog digitalnog tržišta.
7. PRIMA NA ZNANJE trenutačna zbivanja na razini Unije usmjerena na podizanje razine kibersigurnosti povezanih uređaja, posebno u pogledu nedavnih inicijativa Komisije čiji je cilj u kratkom roku odgovoriti na aspekte kibersigurnosti u relevantnim pravnim aktima, primjerice aktima u okviru novog zakonodavnog okvira (NZO), posebno Direktivi 2014/53/EU (Direktiva o radijskoj opremi). ISTIČE važnost procjene potrebe za horizontalnim zakonodavstvom, među ostalim kojim se utvrđuju nužni uvjeti za stavljanje na tržište, kako bi se dugoročno odgovorilo na sve relevantne aspekte kibersigurnosti povezanih uređaja, kao što su dostupnost, cjelovitost i povjerljivost. U tom pogledu POZDRAVLJA raspravu usmjerenu na razmatranje područja primjene takvog zakonodavstva i njegovih poveznica s okvirom za kibersigurnosnu certifikaciju, kako je definiran u Aktu o kibersigurnosti (AOK), s ciljem podizanja razine sigurnosti unutar jedinstvenog digitalnog tržišta.
8. ISTIČE da bi kibersigurnosne zahtjeve trebalo definirati u skladu s relevantnim zakonodavstvom Unije, uključujući AOK, NZO, Uredbu o europskoj normizaciji i moguće buduće horizontalno zakonodavstvo, kako bi se izbjegle nejasnoće i rascjepkanost zakonodavstva.

9. PREPOZNAJE važnu ulogu svih dionika, posebno proizvođača, u povećavanju razine kibersigurnosti povezanih uređaja na jedinstvenom digitalnom tržištu te stoga POZIVA na koordinaciju i blisku suradnju sa svim relevantnim javnim i privatnim dionicima, također u pogledu mogućeg budućeg horizontalnog zakonodavstva.
- 9.a POZDRAVLJA aktualni rad pod vodstvom ENISA-e na donošenju nacрта prvih programa kibersigurnosne certifikacije EU-a, točnije predložene zajedničke kriterije Europske unije i predložene programe usluga računalstva u oblaku. Ti će programi biti važni kao temelj za certifikaciju povezanih uređaja.
10. NAGLAŠAVA da bi se svakim dodatnim programom certifikacije za povezane uređaje i s njima povezane usluge, koji bi bili utvrđeni u kontinuiranom programu rada Unije i definirani na temelju AOK-a, trebalo odrediti kako bi se primjenjivi sigurnosni zahtjevi na odgovarajućoj jamstvenoj razini trebali ispuniti na temelju specifičnih europskih i međunarodno priznatih normi, bez obzira na sektor u kojem će se proizvod upotrebljavati, te koje ispitne specifikacije, potvrde itd. treba primjenjivati.
11. POTVRĐUJE da bi za certifikaciju povezanih uređaja bili potrebni relevantne norme, standardi ili tehničke specifikacije za kibersigurnosne evaluacije na temelju AOK-a. Stoga NAGLAŠAVA potrebu za uspostavom kibersigurnosnih normi, standarda ili tehničkih specifikacija za povezane uređaje i PREPORUČUJE da se pojačaju naponi koje s tim u vezi poduzimaju europske organizacije za normizaciju. Istodobno PREPOZNAJE kibersigurnosnu normu ETSI EN 303 645 za potrošačke uređaje interneta stvari kao važan korak u tom smjeru.

12. POZIVA Komisiju da razmotri zahtjev za [...] prijedloge programâ kibersigurnosne certifikacije za povezane uređaje i povezane usluge na temelju kontinuiranog programa rada Unije, trenutačno u izradi, imajući u najvećoj mogućoj mjeri u vidu horizontalne europske programe kibersigurnosne certifikacije, koji su trenutačno u procesu pripreme. Na dobrovoljnoj osnovi takav će program proizvođačima tih proizvoda omogućiti da promiču proizvode s procijenjenom jamstvenom razinom.
13. POZIVA na raspravu o načinu na koji bi se cilj kibersigurnosti mogao integrirati u buduće horizontalno zakonodavstvo koje se odnosi na kibersigurnosne rizike u vezi s povezanim uređajima i istodobno NAPOMINJE da je potrebno razmotriti prilagodbu bitnih zahtjeva odgovarajućih direktiva o NZO-u, ako je to primjereno.
14. POTIČE Komisiju da, prema potrebi, ocijeni i komplementarne sektorske propise kojima bi se trebala utvrditi razina kibersigurnosti koju bi povezani uređaj trebao doseći radi osiguravanja uspostave posebnih zahtjeva u vidu sigurnosti i privatnosti za takve uređaje s višim sigurnosnim rizicima.
15. ISTIČE potrebu za poboljšanjem kvalitete života i dobrobiti europskih građana te poticanjem povjerenja u jedinstveno digitalno tržište. Sigurnost i privatnost naših društava ključne su za očuvanje naših temeljnih vrijednosti Unije. Stoga NAGLAŠAVA da je potrebno nadovezati se na okvir iz AOK-a kako bi se uskladili sigurnosni zahtjevi prema različitim jamstvenim razinama u svim sektorima NZO-a radi izbjegavanja fragmentacije i višestrukih provjera identičnih zahtjeva te radi pružanja jednakih uvjeta tržišnog natjecanja i inovacija u cijeloj Europskoj uniji.

16. POZIVA Komisiju, Agenciju EU-a za kibersigurnost (ENISA), Odbor za ocjenjivanje sukladnosti i nadzor tržišta telekomunikacija i Europsku skupinu za kibersigurnosnu certifikaciju (ECCG) da aktivno sudjeluju u toj inicijativi jačanja jedinstvenog digitalnog tržišta i unaprjeđenja povjerenja u proizvode, usluge i procese IKT-a za povezane uređaje osiguravanjem privatnosti i kibersigurnosti te da olakšaju veću globalnu konkurentnost industrije interneta stvari Unije osiguravanjem najviših standarda otpornosti, sigurnosti i zaštite.
17. ISTIČE u tom kontekstu potrebu za potporom MSP-ovima kao ključnoj sastavnici europskog kibersigurnosnog ekosustava te POTIČE MSP-ove da sudjeluju u svim pokrenutim javnim savjetovanjima i aktivnostima normizacije kako bi se uzeo u obzir njihov vrijedan i važan doprinos tome da kibersigurnost postane dostupan cilj i konkurentna prednost na europskom tržištu.
18. NAPOMINJE da bi obveza osiguravanja kibersigurnosti i privatnosti tijekom cijelog životnog ciklusa proizvoda i duž njegova opskrbnog lanca mogla imati pozitivan učinak na okolišni otisak tehnološkog sektora usmjeravanjem proizvođača prema pametnim i održivim razvojnim i proizvodnim procesima, čime bi se smanjila količina elektroničkog otpada povezanog s odlaganjem povezanih uređaja.
