Eiropas Savienības
Padome

Briselē, 2022. gada 16. septembrī
(OR. en)

Starpiestāžu lieta:
2022/0272(COD)

12429/22
ADD 6

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

PAVADVĒSTULE

Sūtītājs:	Eiropas Komisijas ģenerālsekretāre, parakstījusi direktore *Martine DEPREZ*
Saņemšanas datums:	2022. gada 15. septembris
Saņēmējs:	Padomes Ģenerālsekretariāts
K-jas dok. Nr.:	SWD(2022) 283 final
Temats:	KOMISIJAS DIENESTU DARBA DOKUMENTS IETEKMES NOVĒRTĒJUMA KOPSAVILKUMA ZIŅOJUMS par Eiropas kibernoturības aktu Pavaddokuments dokumentam Priekšlikums Eiropas Parlamenta un Padomes Regula par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulu (ES) 2019/1020

Pielikumā ir pievienots dokuments SWD(2022) 283 *final*.

Pielikumā: SWD(2022) 283 *final*

EIROPAS
KOMISIJA

Briselē, 15.9.2022.
SWD(2022) 283 final

KOMISIJAS DIENESTU DARBA DOKUMENTS

IETEKMES NOVĒRTĒJUMA KOPSAVILKUMA ZIŅOJUMS

par Eiropas kibernoturības aktu

Pavaddokuments dokumentam

Priekšlikums
Eiropas Parlamenta un Padomes Regula

par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulu (ES) 2019/1020

{COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 282 final}

Kopsavilkums (maks. 2 lappuses)

Kibernoturības akta (KNA) ietekmes novērtējums

A. Rīcības nepieciešamība

Kāda ir problēmas būtība un kāpēc problēma ir nozīmīga ES mērogā?

Pret aparatūras un programmatūras produktiem bieži tiek īstenoti sekmīgi kiberuzbrukumi, kuru dēļ kibernoziedzības radītās ikgadējās izmaksas pēc aplēsēm pasaulē 2021. gadā sasniedza 5,5 triljonus EUR. Šādus produktus skar divas lielas problēmas, kas rada papildu izmaksas lietotājiem un sabiedrībai: 1) zems kiberdrošības līmenis, ko atspoguļo plaši izplatītas ievainojamības un nepietiekama un nekonsekventa drošības atjauninājumu nodrošināšana to novēršanai, un 2) nepietiekama lietotāju izpratne un piekļuve informācijai, kas neļauj lietotājiem izvēlēties produktus ar atbilstošām kiberdrošības īpašībām vai tos izmantot drošā veidā.

Produktu ar digitāliem elementiem kiberdrošībai ir izteikta pārrobežu dimensija, jo vienā valstī ražoti produkti bieži tiek lietoti visā iekšējā tirgū. Turklāt incidenti, kas sākotnēji ietekmē vienu vienību vai vienu dalībvalsti, bieži vien dažās minūtēs izplatās visā iekšējā tirgū.

Lai gan spēkā esošos iekšējā tirgus tiesību aktus piemēro noteiktiem produktiem ar digitāliem elementiem, uz lielāko daļu aparatūras un programmatūras produktu patlaban neattiecas neviens ES tiesību akts, ar kuru tiktu risināta šo produktu kiberdrošība. Konkrēti pašreizējais ES tiesiskais regulējums nerisina neiegultas programmatūras kiberdrošību, neskatoties uz to, ka uzbrukumi kiberdrošībai arvien vairāk tiek vērsti uz šo produktu ievainojamībām, radot būtiskas sociālās un ekonomiskās izmaksas. Jaunākie piemēri ir spiegprogrammatūra *Pegasus*, kas izmantoja mobilo tālruņu ievainojamības, vai izspiedējvīruss *WannaCry*, kas izmantoja *Windows* ievainojamības, ietekmējot datorus visā pasaulē.

Kas būtu jāpanāk?

Tika noteikti šādi divi galvenie mērķi, kuri vērsti uz pareizas iekšējā tirgus darbības nodrošināšanu: 1) radīt apstākļus, lai tiktu izstrādāti droši produkti ar digitāliem elementiem, nodrošinot, ka aparatūras un programmatūras produkti tirgū tiek laisti ar mazāk ievainojamībām un ka ražotājiem ir nopietna attieksme pret drošību visā produkta aprites ciklā; un 2) radīt apstākļus, kas lietotājiem, izvēloties un lietojot produktus ar digitāliem elementiem, dod iespēju ņemt vērā kiberdrošību. Tika noteikti četri konkrētie mērķi: i) nodrošināt, ka ražotāji, sākot no projektēšanas un izstrādes posma, kā arī visā aprites ciklā uzlabo produktu ar digitāliem elementiem drošību; ii) nodrošināt saskaņotu kiberdrošības satvaru, sekmējot aparatūras un programmatūras ražotāju atbilstību; iii) uzlabot produktu ar digitāliem elementiem drošības īpašību pārredzamību un iv) sniegt iespēju uzņēmumiem un patērētājiem droši lietot produktus ar digitāliem elementiem.

Kāda ir ES līmeņa rīcības pievienotā vērtība (subsidiaritāte)?

Kiberdrošības izteiktais pārrobežu raksturs un pieaugošais to incidentu skaits, kuru ietekme izvēršas pāri robežām, starp dažādām nozarēm un produktiem, nozīmē, ka dalībvalstis vienas pašas nevar efektīvi sasniegt mērķus. Ņemot vērā produktu ar digitāliem elementiem tirgu globālo raksturu, dalībvalstis savā teritorijā attiecībā uz vienu un to pašu produktu ar digitāliem elementiem saskaras ar vieniem un tiem pašiem riskiem. Jauns sadrumstalots regulējums, ko veido potenciāli atšķirīgi valstu noteikumi, arī rada risku, ka varētu tikt kavēts atvērts un konkurētspējīgs vienotais tirgus attiecībā uz produktiem ar digitāliem elementiem. Tāpēc, lai palielinātu lietotāju uzticēšanos un ES produktu ar digitāliem elementiem pievilcību, ir vajadzīga vienota rīcība ES līmenī. Tā nāktu par labu arī iekšējam tirgum, nodrošinot juridisko noteiktību un panākot vienlīdzīgus konkurences apstākļus produktu ar digitāliem elementiem

ražotājiem.

B. Risinājumi

Kādi ir risinājumu varianti izvirzīto mērķu sasniegšanai? Vai ir kāds vēlamākais risinājums? Iemesli (ja risinājuma nav)

Tika analizēti četri politikas risinājumu varianti un saistītie apakšvarianti, kas pārsniedz *status quo*: 1) ieteikuma tiesību pieeja un brīvprātīgi pasākumi; 2) *ad hoc* regulatīva intervence attiecībā uz konkrētu produktu saistībā ar materiālu produktu ar digitāliem elementiem un attiecīgās iegultās programmatūras kiberdrošību; 3) jaukta pieeja, kas ietver horizontālus obligātus noteikumus attiecībā uz materiālu produktu ar digitāliem elementiem un attiecīgās iegultās programmatūras kiberdrošību, kā arī vairāku posmu pieeju neiegultai programmatūrai, ar diviem atbilstības novērtēšanas apakšvariantiem; un 4) horizontāla regulatīva intervence, ar ko ievieš kiberdrošības prasības plašam produktu ar digitāliem elementiem klāstam, arī neiegultai programmatūrai, ar apakšvariantiem attiecībā uz darbības jomu un atbilstības novērtējumu.

Ietekmes novērtējumā tika secināts, ka **vēlamais risinājums** ir 4. risinājums, kas aptver visus produktus ar digitāliem elementiem un paredz obligātu trešo personu veiktu novērtējumu kritiski svarīgu produktu gadījumā, pamatojoties uz novērtējumu par efektivitāti attiecībā pret konkrētajiem mērķiem, izmaksu lietderību salīdzinājumā ar ieguvumiem un saskaņotību.

Dažādu ieinteresēto personu viedokļi. Kuru risinājumu katra no ieinteresētajām personām atbalsta?

Kad sabiedriskās apspriešanas respondentiem tika lūgts novērtēt politikas intervences pasākumu efektivitāti, tie atzina, ka 4. risinājums būtu visefektīvākais pasākums (4,08 skalā no 1 līdz 5). Respondenti bija patērētāju organizācijas (5,00), respondenti, kas sevi identificē kā lietotājus (4,22), paziņotās struktūras (4,17), tirgus uzraudzības iestādes (5,00) un produktu ar digitāliem elementiem ražotāji (3,85), to vidū mazie un vidējie (4,05).

C. Vēlamā risinājuma ietekme

Kādus ieguvumus nodrošinās vēlamais risinājums (ja tāds ir, pretējā gadījumā — galvenie risinājumi)?

Vēlamais risinājums sniegtu ievērojamu labumu dažādām ieinteresētajām personām. Uzņēmumiem tas novērstu atšķirīgus drošības noteikumus attiecībā uz produktiem ar digitāliem elementiem un samazinātu atbilstības nodrošināšanas izmaksas attiecībā uz saistītajiem kiberdrošības tiesību aktiem. Tas samazinātu kiberincidentu skaitu, incidentu risināšanas izmaksas un kaitējumu reputācijai. Tiek lēsts, ka visā ES šī iniciatīva varētu par aptuveni 180–290 miljardiem EUR gadā samazināt izmaksas, ko rada incidenti, kas skar uzņēmumus. Turklāt iniciatīva palielinātu apgrozījumu, jo produkti ar digitāliem elementiem tiktu izmantoti arvien vairāk. Tas arī uzlabotu uzņēmumu reputāciju pasaulē, izraisot pieprasījumu ārpus ES. Galalietotāju gadījumā vēlamais risinājums palielinātu drošības īpašību pārredzamību un atvieglotu produktu ar digitāliem elementiem izmantošanu. Patērētāji un iedzīvotāji iegūtu arī no tā, ka tiktu labāk aizsargātas viņu pamattiesības, piemēram, privātums un datu aizsardzība.

Cik izmaksās vēlamākais risinājums (ja tāds ir, pretējā gadījumā — galvenie risinājumi)?

Vēlamais risinājums palielinātu atbilstības nodrošināšanas un izpildes izmaksas uzņēmumiem, paziņotajām struktūrām un publiskajām iestādēm, to vidū paziņošanas, akreditācijas un tirgus uzraudzības iestādēm. Programmatūras izstrādātājiem un aparatūras ražotājiem tas palielinās tiešās atbilstības

nodrošināšanas izmaksas saistībā ar jaunām kiberdrošības prasībām, atbilstības novērtējumu, dokumentēšanas un ziņošanas pienākumiem, tādējādi kopējās atbilstības nodrošināšanas izmaksas sasniegtu aptuveni 29 miljardus EUR attiecībā pret produktu ar digitāliem elementiem tirgus vērtību, kas apgrozījuma izteiksmē ir lēsta līdz 1485 miljardiem EUR. Galalietotājiem, to vidū komerciālajiem galalietotājiem, patērētājiem un iedzīvotājiem, var nākties maksāt augstāku cenu par produktiem ar digitāliem elementiem. Tomēr šīs izmaksas būtu jāaplūko, ņemot vērā iepriekš aprakstītos būtiskos ieguvumus. Paredzams, ka paziņoto struktūru papildu izmaksas kompensēs apgrozījuma pieaugums.
Ietekme uz MVU un konkurētspēju
Jaunās prasības ietekmēs MVU gan kā ražotājus, gan kā galalietotājus. Atbilstības nodrošināšanas izmaksu ziņā MVU principā tiktu ietekmēti vairāk nekā lielie uzņēmumi, kuriem parasti ir labāki apjomradīti ietaupījumi un lielāka izpratne par kiberdrošību. Tomēr MVU gūtu lielu labumu no iniciatīvas, jo kiberdrošība, kas iegulta produktos ar digitāliem elementiem, radītu būtiskus izmaksu ietaupījumus MVU kā lietotājiem. Kā ražotāji MVU gūtu labumu no lielākas galalietotāju uzticības un jauniem klientiem. Netraucēta piekļuve iekšējam tirgum un tirgus sadrumstalotības samazināšana var būt vēl izdevīgāka MVU, kas ir mazāk sagatavoti dažādu normatīvo prasību izpildei. Uzsverot samērīgas pieejas un atbalsta pasākumu nepieciešamību, MVU kopumā atbalstīja vienlīdzīgus konkurences apstākļus visiem uzņēmumiem un neuzskatīja, ka horizontālo obligāto prasību scenārijā tie būtu nelabvēlīgākā situācijā nekā lielāki uzņēmumi.
Vai tiks būtiski ietekmēts valstu budžets un pārvaldes iestādes?
Iniciatīva ietekmēs valsts iestādes, piemēram, valsts paziņojošās iestādes, akreditācijas iestādes un tirgus uzraudzības iestādes, kuru pienākums ir uzraudzīt un īstenot ierosinātos pasākumus. Šīm iestādēm būs papildu pielāgošanas (piemēram, apmācības un cilvēkresursu) un izpildes izmaksas, lai ņemtu vērā jaunās prasības. Tomēr akreditācijas struktūru iztērētos resursus kompensē un lielā mērā sedz atbilstības novērtēšanas struktūras, pērkot akreditācijas pakalpojumus.
Cita paredzama būtiska ietekme
Cita būtiska negatīva ietekme nav paredzama. Vēlamais politikas risinājums palīdzētu samazināt incidentu skaitu un smagumu, ieskaitot persondatu aizsardzības pārkāpumus, un tam būtu pozitīva sociālā ietekme, piemēram, samazināts kibernoziedzības apmērs. Visticamāk, pieaugs drošības speciālistu pieprasījums un samazināsies kiberdrošības informācijas asimetrija.
Proporcionalitāte?
Vēlamais politikas risinājums nepārsniedz to, kas ir nepieciešams konkrēto mērķu apmierinošai sasniegšanai. Intervence nodrošinātu, ka produkti ar digitāliem elementiem tiek aizsargāti visā to aprites ciklā un proporcionāli attiecīgajiem riskiem.
D. Turpmākā rīcība
Politikas pārskatīšanas termiņš
[36 mēnešus] pēc šīs regulas piemērošanas dienas un pēc tam reizi četros gados Komisija iesniedz Eiropas Parlamentam un Padomei ziņojumu par šīs iniciatīvas izvērtēšanu un pārskatīšanu.