Eiropas Savienības
Padome

Briselē, 2020. gada 18. decembrī
(OR. en)

14150/20
ADD 3

Starpiestāžu lieta:
2020/0359(COD)

CYBER 281
JAI 1119
DATAPROTECT 155
TELECOM 270
MI 581
CSC 368
CSCI 97

PAVADVĒSTULE

Sūtītājs:	Eiropas Komisijas ģenerālsekretāre, parakstījusi direktore *Martine DEPREZ*
Saņemšanas datums:	2021. gada 16. janvāris
Saņēmējs:	Eiropas Savienības Padomes ģenerālsekretārs *Jeppe TRANHOLM-MIKKELSEN*
K-jas dok. Nr.:	SWD(2020) 344 final
Temats:	KOMISIJAS DIENESTU DARBA DOKUMENTS IETEKMES NOVĒRTĒJUMA KOPSAVILKUMA ZIŅOJUMS Pavaddokuments dokumentam Priekšlikums Eiropas Parlamenta un Padomes Direktīvai, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148

Pielikumā ir pievienots dokuments SWD(2020) 344 *final*.

Pielikumā: SWD(2020) 344 *final*

EIROPAS
KOMISIJA

Briselē, 16.12.2020.
SWD(2020) 344 final

KOMISIJAS DIENESTU DARBA DOKUMENTS

IETEKMES NOVĒRTĒJUMA KOPSAVILKUMA ZIŅOJUMS

Pavaddokuments dokumentam

Priekšlikums Eiropas Parlamenta un Padomes Direktīvai,

ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148

{COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 345 final}

Kopsavilkuma lapa

Ietekmes novērtējums par *2016. gada 6. jūlija Direktīvas (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (turpmāk "TID direktīva") pārskatīšanu*

A. Rīcības nepieciešamība

Problēmas būtība un nozīme ES mērogā

Neraugoties uz tās ievērojamiem sasniegumiem, TID direktīva, kas lika pamatus ievērojamām izmaiņām domāšanas veidā un institucionālajā un regulatīvajā pieejā kiberdrošībai daudzās dalībvalstīs, līdz šim ir arī apliecinājusi savus ierobežojumus. Sabiedrības digitālā pārveide (ko pastiprināja Covid-19 krīze) ir paplašinājusi draudu ainu un rada jaunas problēmas, kurām ir vajadzīgi pielāgoti un inovatīvi reaģēšanas pasākumi. Kiberuzbrukumu skaits turpina pieaugt, un no avotiem gan ES, gan ārpus tās tiek vērsti arvien sarežģītāki uzbrukumi.

Pamatojoties uz TID direktīvas darbības izvērtējumu, ietekmes novērtējumā tika identificētas šādas problēmas: uzņēmumu, kas darbojas ES, zemais kibernoturības līmenis; neviendabīgā noturība starp dalībvalstīm un nozarēm, kā arī kopējās situācijas apzināšanās zemais līmenis un kopīgas reaģēšanas uz krīzi trūkums. Piemēram, dažu šo problēmu un veicinošo faktoru rezultātā ir radušās situācijas, kurās TID direktīvas darbības jomā nav lielās slimnīcas, un tāpēc tām nav jāīsteno izrietošie drošības pasākumi, savukārt citā dalībvalstī TID drošības prasības attiecas gandrīz uz katru slimnīcu valstī.

Sasniedzamie mērķi

TID pārskatīšanai ir trīs vispārīgi mērķi:

1. **paaugstināt Eiropas Savienībā darbojošos uzņēmumu visaptveroša kopuma kibernoturības līmeni visās būtiskajās nozarēs,** ieviešot noteikumus, kas nodrošina, ka visām publiskajām un privātajām vienībām iekšējā tirgū, kuras pilda ekonomikai un visai sabiedrībai svarīgas funkcijas, ir jāveic atbilstoši kiberdrošības pasākumi;
2. **mazināt noturības atšķirības visā iekšējā tirgū nozarēs, uz kurām direktīva jau attiecas,** vēl vairāk saskaņojot 1) *de-facto* darbības jomu, 2) drošības un incidentu paziņošanas prasības, 3) noteikumus, kas reglamentē uzraudzību un izpildi valsts līmenī, un 4) kompetento iestāžu spējas dalībvalstīs;
3. **uzlabot kopējās situācijas apzināšanās līmeni un kolektīvo spēju sagatavoties un reaģēt,** veicot pasākumus, lai palielinātu uzticēšanās līmeni starp kompetentajām iestādēm, apmainoties ar plašāku informāciju un nosakot noteikumus un procedūras plašapmēra incidenta vai krīzes gadījumā.

ES līmeņa rīcības pievienotā vērtība (subsidiaritāte)

Kiberdrošības noturība visā Savienībā nevar būt efektīva, ja attiecībā uz to tiek īstenotas atšķirīgas valstu vai reģionālās pieejas. TID direktīva pievērsās šim trūkumam, nosakot satvaru tīklu un informācijas sistēmu drošībai valstu un Savienības līmenī. Tomēr tās transponēšanā un īstenošanā arī atklājās raksturīgi trūkumi saistībā ar konkrētiem noteikumiem vai pieejām, piemēram, neskaidrais TID direktīvas darbības jomas norobežojums. Turklāt kopš Covid-19 krīzes Eiropas ekonomika ir kļuvusi tik atkarīga no tīklu un informācijas sistēmām kā nekad iepriekš, un nozares un pakalpojumi kļūst arvien vairāk savstarpēji atkarīgi. Tāpēc pirmā TID direktīvas periodiskā pārskatīšana radīja iespēju turpmākai ES rīcībai. ES iejaukšanos, kas pārsniedz pašreizējos TID direktīvas pasākumus, pamato galvenokārt šādi faktori:

i) problēmas pārrobežu raksturs; ii) iespēja, ka ar ES rīcību tiks uzlabota un veicināta efektīva valstu politika; iii) saskaņotu un sadarbīgu TID politikas darbību ieguldījums efektīvā datu un privātuma aizsardzībā.

B. Risinājumi

Risinājumu varianti izvirzīto mērķu sasniegšanai. Vēlamais risinājums (ja ir). Iemesli (ja nav)

Ietekmes novērtējumā tika analizēti četri politikas risinājumi: 0) līdzšinējā stāvokļa saglabāšana; 1) neleģislatīvi pasākumi, lai pielāgotu transponēšanu; 2) ierobežotas izmaiņas TID direktīvā turpmākai saskaņošanai; 3) sistēmiskas un strukturālas izmaiņas TID direktīvā. Risinājums Nr. 1 tika atmests jau agrīnā posmā, jo tas būtiski neatšķiras no līdzšinējā stāvokļa saglabāšanas. Ietekmes novērtējumā ir secināts, ka **vēlamais risinājums** ir 3. risinājums (t. i., **sistēmiskas un strukturālas izmaiņas TID regulējumā**), jo tas paredzētu stingrāku pieejas novirzīšanu uz to, lai aptvertu plašāku tautsaimniecību segmentu visā Savienībā, tomēr ar mērķtiecīgāku uzraudzību, kas samērīgi vērsts uz lielajiem un galvenajiem uzņēmumiem, vienlaikus skaidri nosakot piemērošanas jomu. Tas arī racionalizētu un turpmāk saskaņotu ar drošību saistītos pienākumus uzņēmumiem, radītu efektīvāku vidi operatīvajiem aspektiem, kā arī radītu skaidru pamatu attiecīgo dalībnieku dalītiem pienākumiem un pārskatatbildībai un stimulētu informācijas apmaiņu.

Ieinteresēto personu viedokļi. Atbalsts konkrētiem risinājumiem

Lielākā daļa kompetento iestāžu un uzņēmumu pauda atbalstu TID direktīvas pārskatīšanai. Vairākās apspriešanās tie norādīja, ka pārskatītai TID direktīvai būtu jāaptver papildu (apakš-)nozares, jāpielāgo vai jāracionalizē papildu drošības pasākumi un ziņošanas pienākumi. Ieinteresētās personas arī izteica atbalstu jaunām koncepcijām vai ar politiku saistītiem pasākumiem, kas ir tikai daļa no vēlamā risinājuma (piemēram, piegādes ķēdes drošības politika, operatīvā ES krīžu pārvaldības satvara institucionalizācija).

C. Vēlamā risinājuma ietekme

Vēlamā risinājuma (ja tāds ir; pretējā gadījumā — galveno risinājumu) nodrošinātie ieguvumi

Vēlamais risinājums nodrošinātu būtiskus ieguvumus — aplēses, kas veiktas, pamatojoties uz ekonomisko modelēšanu, kura izstrādāta atbalsta pētījumā TID regulējuma pārskatīšanai, liecina, ka vēlamais risinājums varētu samazināt kiberdrošības incidentu izmaksas par 11,3 miljardiem EUR.

Nozaru tvērums tiktu ievērojami palielināts atbilstoši TID regulējumam, taču papildus minētajiem ieguvumiem arī slogs, ko var radīt TID prasības, jo īpaši no uzraudzības viedokļa, būtu līdzsvarots gan jaunām vienībām, kas jāaptver, gan kompetentajām iestādēm. Proti, ar jauno TID regulējumu tiktu izveidota divslāņu pieeja, koncentrējoties uz lielām un svarīgām vienībām, un uzraudzības režīma diferencēšana, kas ļauj piemērot tikai *ex post* uzraudzību (t. i., ar atpakaļejošu spēku un bez vispārēja pienākuma sistemātiski dokumentēt atbilstību) lielam skaitam vienību, jo īpaši vienības, ko uzskata par "svarīgām", bet ne "būtiskām".

Kopumā vēlamais politikas risinājums radītu efektīvus kompromisus un sinerģijas, jo tam ir no visiem analizētajiemm politikas risinājumiem vislielākais potenciāls nodrošināt uzlabotu un saskaņotu galveno vienību kibernoturības līmeni visā Savienībā, galu galā radot izmaksu ietaupījumus gan uzņēmumiem, gan sabiedrībai.

Vēlamā risinājuma (ja tāds ir, pretējā gadījumā — galveno risinājumu) izmaksas

Vēlamais politikas risinājums radītu konkrētas atbilstības nodrošināšanas un izpildes izmaksas

attiecīgajām dalībvalstu iestādēm (tika aplēsts kopējais palielinājums par aptuveni 20–30 % no resursiem). Tomēr jaunais regulējums arī radītu ievērojamus ieguvumus, jo uzlabotos priekšstats par galvenajiem uzņēmumiem un mijiedarbība ar tiem, uzlabotos pārrobežu operatīvā sadarbība, kā arī savstarpējā palīdzība un salīdzinošās izvērtēšanas mehānismi. Tas vispārēji palielinātu kiberdrošības spējas dalībvalstīs.

Tiek lēsts, ka uzņēmumiem, uz kuriem tiktu attiecināts TID regulējums, to pašreizējie izdevumi IKT drošībai būtu jāpalielina par ne vairāk kā 22 % pirmajos gados pēc jaunā TID regulējuma ieviešanas (uzņēmumiem, uz kuriem jau attiecas pašreizējās TID direktīvas darbība joma, tie būtu 12 %). Tomēr šis IKT drošības izdevumu vidējais palielinājums radītu samērīgu ieguvumu no šādiem ieguldījumiem, jo īpaši tādēļ, ka ievērojami samazinātos kiberdrošības incidentu izmaksas (tiek lēstas 11,3 miljardu EUR apmērā desmit gadu laikposmā).

Ietekme uz MVU un konkurētspēju

Atbilstīgi vēlamajam risinājumam TID regulējums neattiektos uz mazajiem uzņēmumiem un mikrouzņēmumiem. Attiecībā uz vidējiem uzņēmumiem ir gaidāms, ka IKT drošības izdevumu līmenis palielināsies pirmajos gados pēc jaunā TID regulējuma ieviešanas. Tajā pašā laikā kiberdrošības prasību līmeņa paaugstināšana šīm vienībām arī stimulētu to kiberdrošības spējas un palīdzētu uzlabot to IKT riska pārvaldību.

Nozīmīga ietekme uz valstu budžetiem un valsts pārvaldes iestādēm

Būtu ietekme uz valstu budžetiem un valsts pārvaldi — tiek lēsts, ka īstermiņā un vidējā termiņā palielinājums būtu aptuveni 20–30 % no resursiem.

Cita nozīmīga ietekme

Cita būtiska negatīva ietekme nav paredzama. Paredzams, ka vēlamais politikas risinājums radīs stabilākas kiberdrošības spējas un attiecīgi radīs ievērojamāku mazinošu ietekmi uz incidentu, tostarp datu aizsardzības pārkāpumu, skaitu un smagumu. Tam arī, visticamāk, būs pozitīva ietekme uz vienlīdzīgu konkurences apstākļu nodrošināšanu dalībvalstīs visām vienībām, uz kurām attiecas TID regulējums, un tas mazinās kiberdrošības informācijas asimetriju.

Proporcionalitāte

Vēlamais politikas risinājums nepārsniedz to, kas ir nepieciešams konkrēto mērķu apmierinošai sasniegšanai. Paredzētā drošības pasākumu un ziņošanas pienākumu saskaņošana un racionalizācija ir saistīta ar dalībvalstu un uzņēmumu lūgumiem uzlabot pašreizējo regulējumu.

D. Turpmākā rīcība

Politikas pārskatīšanas termiņš

Pirmā pārskatīšana notiktu, kad no tiesību akta stāšanās spēkā būtu pagājuši 54 mēneši. Komisija Eiropas Parlamentam un Padomei ziņotu par tā pārskatīšanu. Sagatavošanās pārskatīšanai notiktu ar *ENISA* un sadarbības grupas atbalstu.