Svet
Evropske unije

Bruselj, 18. december 2020
(OR. en)

Medinstitucionalna zadeva:
2020/0359(COD)

14150/20
ADD 3

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

SPREMNI DOPIS

Pošiljatelj:	za generalno sekretarko Evropske komisije: direktorica Martine DEPREZ
Datum prejema:	16. december 2020
Prejemnik:	generalni sekretar Sveta Evropske unije Jeppe TRANHOLM-MIKKELSEN
Št. dok. Kom.:	SWD(2020) 344 final
Zadeva:	DELOVNI DOKUMENT SLUŽB KOMISIJE POVZETEK POROČILA O OCENI UČINKA Spremni dokument k predlogu direktive Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148

Delegacije prejmejo priloženi dokument SWD(2020) 344 final.

Priloga: SWD(2020) 344 final

EVROPSKA
KOMISIJA

Bruselj, 16.12.2020
SWD(2020) 344 final

DELOVNI DOKUMENT SLUŽB KOMISIJE

POVZETEK POROČILA O OCENI UČINKA

Spremni dokument k

predlogu direktive Evropskega parlamenta in Sveta

o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148

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

Povzetek

Ocena učinka *pregleda Direktive (EU) 2016/1148 z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (v nadaljnjem besedilu: direktiva o varnosti omrežij in informacijskih sistemov)*

A. Potreba po ukrepanju

V čem je težava in zakaj je to težava na ravni EU?

Kljub pomembnim dosežkom direktive o varnosti omrežij in informacijskih sistemov, ki je utrla pot do velike spremembe v miselnosti ter institucionalnem in regulativnem pristopu h kibernetski varnosti v številnih državah članicah, so se doslej pokazale tudi njene omejitve. Z digitalno preobrazbo družbe (ki jo je okrepila kriza zaradi COVID-19) se je okolje groženj razširilo in nastajajo novi izzivi, ki zahtevajo prilagojene in inovativne odzive. Število kibernetskih napadov se še naprej povečuje, vse bolj izpopolnjeni napadi pa prihajajo iz različnih virov znotraj EU in zunaj nje.

Na podlagi ocene delovanja direktive o varnosti omrežij in informacijskih sistemov so bile v oceni učinka opredeljene naslednje težave: nizka raven kibernetske odpornosti podjetij, ki delujejo v EU; neskladna odpornost po državah članicah in sektorjih ter nizka raven skupnega situacijskega zavedanja in pomanjkanje skupnega odzivanja na krize. Zaradi nekaterih od teh težav in dejavnikov obstajajo na primer primeri, ko večje bolnišnice v državi članici ne spadajo na področje uporabe direktive o varnosti omrežij in informacijskih sistemov in jim zato ni treba izvajati varnostnih ukrepov, ki izhajajo iz nje, medtem ko v drugi državi članici za skoraj vsako bolnišnico v državi veljajo zahteve glede varnosti omrežij in informacijskih sistemov.

Kaj bi bilo treba doseči?

V pregledu direktive o varnosti omrežij in informacijskih sistemov so predvideni trije splošni cilji:

1. **zvišati raven kibernetske odpornosti obsežne skupine podjetij, ki delujejo v Evropski uniji, v vseh ustreznih sektorjih** z uvedbo pravil, ki zagotavljajo, da so vsi javni in zasebni subjekti na notranjem trgu, ki opravljajo pomembne funkcije za gospodarstvo in družbo kot celoto, zavezani sprejeti ustrezne ukrepe za kibernetsko varnost;
2. **zmanjšati razlike v odpornosti na notranjem trgu v sektorjih, ki so že zajeti z Direktivo,** z nadaljnjim usklajevanjem (1) dejanskega področja uporabe, (2) zahtev glede varnosti in poročanja o incidentih, (3) določb, ki urejajo nacionalni nadzor in izvrševanje, ter (4) zmogljivosti pristojnih organov v državah članicah;
3. **izboljšati raven skupnega situacijskega zavedanja in skupne zmogljivosti za pripravo in odzivanje** s sprejetjem ukrepov za povečanje ravni zaupanja med pristojnimi organi in večjo izmenjavo informacij ter določitvijo pravil in postopkov v primeru obsežnega incidenta ali krize.

Kakšna je dodana vrednost ukrepanja na ravni EU (subsidiarnost)?

Kibernetska odpornost v Uniji ne more biti učinkovita, če se k njej zaradi nacionalnih ali regionalnih omejitev pristopa neenotno. V direktivi o varnosti omrežij in informacijskih sistemov so te pomanjkljivosti obravnavane z določitvijo okvira za varnost omrežij in informacijskih sistemov na nacionalni ravni in ravni Unije. Vendar so se z njenim prenosom in izvajanjem pokazale tudi pomanjkljivosti, ki so neločljivo povezane z nekaterimi določbami ali pristopi, kot je nejasna razmejitev področja uporabe direktive o varnosti omrežij in informacijskih sistemov. Poleg tega je evropsko gospodarstvo od začetka krize zaradi COVID-19 postalo bolj odvisno od omrežij in informacijskih

sistemov kot kdaj koli prej, sektorji in storitve pa so vse bolj medsebojno povezani. S prvim rednim pregledom direktive o varnosti omrežij in informacijskih sistemov se je tako ustvarila priložnost za nadaljnje ukrepanje na ravni EU. Ukrepanje EU, ki presega sedanje ukrepe iz direktive o varnosti omrežij in informacijskih sistemov, je upravičeno zlasti zaradi: (i) čezmejne narave problematike; (ii) možnosti, da se z ukrepi EU izboljšajo in olajšajo učinkovite nacionalne politike; (iii) prispevka usklajenih in skupnih ukrepov politike na področju varnosti omrežij in informacijskih sistemov k učinkovitemu varstvu podatkov in zasebnosti.

B. Rešitve

Katere so različne možnosti za dosego ciljev? Ali ima katera od njih prednost? Če ne, zakaj?

V oceni učinka so bile analizirane štiri možnosti politike: (0) ohranjanje sedanjega stanja; (1) nezakonodajni ukrepi za uskladitev prenosa; (2) omejene spremembe direktive o varnosti omrežij in informacijskih sistemov za nadaljnjo harmonizacijo; (3) sistemske in strukturne spremembe direktive o varnosti omrežij in informacijskih sistemov. Možnost 1 je bila v zgodnji fazi zavrnjena, saj se bistveno ne razlikuje od sedanjega stanja. V oceni učinka je bilo ugotovljeno, da je **prednostna možnost** možnost 3 (tj. **sistemske in strukturne spremembe okvira za varnost omrežij in informacijskih sistemov**), saj bi predvidevala temeljitejšo spremembo pristopa k pokrivanju širšega segmenta gospodarstev v Uniji, vendar z bolj osredotočenim nadzorom, sorazmerno usmerjenim v velika in ključna podjetja, in jasno določala področje uporabe. Prav tako bi racionalizirala in dodatno uskladila obveznosti podjetij v zvezi z varnostjo, ustvarila učinkovitejše okolje za operativne vidike ter vzpostavila jasno podlago za deljene obveznosti in odgovornost ustreznih akterjev in spodbudila izmenjavo informacij.

Kakšna so stališča različnih zainteresiranih strani? Kdo podpira katero možnost?

Večina pristojnih organov in podjetij je izrazila podporo reviziji direktive o varnosti omrežij in informacijskih sistemov. Med več posvetovanji so opozorili, da bi morala revidirana direktiva o varnosti omrežij in informacijskih sistemov zajemati dodatne (pod)sektorje ter uskladiti ali racionalizirati nadaljnje varnostne ukrepe in obveznosti poročanja. Zainteresirane strani so izrazile tudi podporo novim konceptom ali ukrepom v zvezi s politiko, ki so le del prednostne možnosti (npr. politike za varnost dobavne verige, institucionalizacija operativnega okvira EU za krizno upravljanje).

C. Učinki prednostne možnosti

Katere so koristi prednostne možnosti (če obstaja, sicer glavnih možnosti)?

Prednostna možnost bi prinesla pomembne koristi: ocene na podlagi ekonomskega modeliranja, razvitega s podporno študijo za pregled varnosti omrežij in informacijskih sistemov, kažejo, da bi prednostna možnost lahko privedla do znižanja stroškov kibernetskih incidentov za 11,3 milijarde EUR.

Sektorsko področje uporabe bi se na podlagi okvira za varnost omrežij in informacijskih sistemov bistveno povečalo, poleg zgoraj navedenih koristi pa bi se za nove subjekte, ki bi bili zajeti, in pristojne organe uravnotežilo tudi breme, ki bi ga lahko ustvarile zahteve glede varnosti omrežij in informacijskih sistemov, zlasti z vidika nadzora. Razlog za to je, da bi bil z novim okvirom za varnost omrežij in informacijskih sistemov vzpostavljen dvostopenjski pristop, s poudarkom na velikih in ključnih subjektih ter razlikovanju nadzorne ureditve, ki omogoča samo naknadni nadzor (tj. reaktiven nadzor brez splošne obveznosti sistematičnega dokumentiranja izpolnjevanja zahtev) velikega števila subjektov, zlasti tistih, ki se štejejo za „pomembne“, vendar ne za „bistvene“.

Na splošno bi prednostna možnost politike privedla do učinkovitih kompromisov in sinergij, z največjim potencialom med vsemi analiziranimi možnostmi politike za zagotovitev višje in usklajene ravni

kibernetske odpornosti ključnih subjektov po vsej Uniji, ki bi sčasoma privedla do prihrankov stroškov za podjetja in družbo.

Kakšni so stroški prednostne možnosti (če obstaja, sicer glavnih možnosti)?

Prednostna možnost politike bi zadevnim organom držav članic povzročila določene stroške za izpolnjevanje obveznosti in izvrševanje (po ocenah naj bi se viri povečali za približno 20–30 %). Vendar bi novi okvir prinesel tudi pomembne koristi z boljšim pregledom ključnih podjetij in sodelovanjem z njimi, okrepljenim čezmejnim operativnim sodelovanjem ter medsebojno pomočjo in mehanizmi medsebojnih strokovnih pregledov. To bi privedlo do splošnega povečanja zmogljivosti za kibernetsko varnost v državah članicah.

Ocenjuje se, da bi morala podjetja, ki bi spadala na področje uporabe okvira za varnost omrežij in informacijskih sistemov, v prvih letih po uvedbi novega okvira za varnost omrežij in informacijskih sistemov svojo sedanjo porabo za varnost IKT povečati za največ 22 % (pri podjetjih, ki že spadajo na področje uporabe sedanje direktive o varnosti omrežij in informacijskih sistemov, bi bilo to povečanje 12-odstotno). Vendar bi to povprečno povečanje porabe za varnost IKT privedlo do sorazmerne koristi takih naložb, zlasti zaradi znatnega znižanja stroškov kibernetskih incidentov (ocenjenega na 11,3 milijarde EUR v desetih letih).

Kakšni so učinki na mala in srednja podjetja ter konkurenčnost?

Mala podjetja in mikropodjetja bi bila pri prednostni možnosti izvzeta iz področja uporabe okvira za varnost omrežij in informacijskih sistemov. Za srednja podjetja se lahko pričakuje, da bi se raven porabe za varnost IKT v prvih letih po uvedbi novega okvira za varnost omrežij in informacijskih sistemov zvišala. Hkrati bi zvišanje ravni varnostnih zahtev za te subjekte tudi zagotovilo spodbude za njihove zmogljivosti za kibernetsko varnost in prispevalo k izboljšanju obvladovanja tveganj na področju IKT.

Ali bo prišlo do pomembnih učinkov na nacionalne proračune in uprave?

To bi imelo učinek na nacionalne proračune in uprave: kratko- in srednjeročno bi bilo po ocenah pričakovati od 20- do 30-odstotno povečanje virov.

Ali bo prišlo do drugih pomembnih učinkov?

Drugi pomembnejši negativni učinki se ne pričakujejo. Prednostna možnost politike naj bi zagotovila zanesljivejše zmogljivosti za kibernetsko varnost in naj bi posledično imela večji blažilni učinek na število in resnost incidentov, vključno s kršitvami varstva podatkov. Verjetno bo imela tudi pozitiven učinek na zagotavljanje enakih konkurenčnih pogojev v državah članicah za vse subjekte, ki spadajo na področje uporabe okvira za varnost omrežij in informacijskih sistemov, ter zmanjšala asimetrijo informacij o kibernetski varnosti.

Sorazmernost?

Prednostna možnost ne presega tistega, kar je potrebno za zadovoljivo doseganje specifičnih ciljev. Predvidena uskladitev in racionalizacija varnostnih ukrepov in obveznosti poročanja se nanašata na zahteve držav članic in podjetij po izboljšanju sedanjega okvira.

D. Spremljanje izvajanja

Kdaj bo politika pregledana?

Prvi pregled bi se izvedel 54 mesecev po začetku veljavnosti pravnega instrumenta. Komisija bi Evropskemu parlamentu in Svetu predložila poročilo o pregledu. Pregled bi bil pripravljen ob podpori agencije ENISA in skupine za sodelovanje.