Vijeće
Europske unije

Bruxelles, 18. prosinca 2020.
(OR. en)

14150/20
ADD 3

Međuinstitucijski predmet:
2020/0359(COD)

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

POPRATNA BILJEŠKA

Od:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
Datum primitka:	16. prosinca 2020.
Za:	Jeppe TRANHOLM-MIKKELSEN, glavni tajnik Vijeća Europske unije
Br. dok. Kom.:	SWD(2020) 344 final
Predmet:	RADNI DOKUMENT SLUŽBI KOMISIJE: SAŽETAK IZVJEŠĆA O PROCJENI UČINKA priložen dokumentu Prijedlog Direktive Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148

Za delegacije se u prilogu nalazi dokument SWD(2020) 344 final.

Priloženo: SWD(2020) 344 final

EUROPSKA
KOMISIJA

Bruxelles, 16.12.2020.
SWD(2020) 344 final

RADNI DOKUMENT SLUŽBI KOMISIJE

SAŽETAK IZVJEŠĆA O PROCJENI UČINKA

priložen dokumentu

Prijedlog Direktive Europskog parlamenta i Vijeća

o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148

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

Sažetak

Procjena učinka revizije Direktive (EU) 2016/1148 od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (dalje u tekstu „Direktiva NIS")

A. Potreba za djelovanjem

O čemu je riječ? Zašto je to problem na razini EU-a?

Bez obzira na važna postignuća Direktive NIS, koja je u mnogim državama članicama bila pokretač znatne promjene načina razmišljanja te institucionalnog i regulatornog pristupa kibersigurnosti, pokazalo se da ima i svoja ograničenja. Digitalna transformacija društva (pojačana krizom uzrokovanom bolešću COVID-19) povećala je prijetnje i dovela do novih izazova koji zahtijevaju prilagođene i inovativne odgovore. Broj kibernapada i dalje raste te sve sofisticiraniji napadi dolaze iz brojnih izvora unutar i izvan EU-a.

Na temelju evaluacije funkcioniranja Direktive NIS, procjenom učinka utvrđeni su sljedeći problemi: niska razina kiberotpornosti poduzeća koja posluju u EU-u; neujednačena otpornost u državama članicama i sektorima; niska razina zajedničke informiranosti o stanju i izostanak zajedničkog odgovora na krizu. Primjerice, nekih od tih problema i pokretača dovode do toga da određene velike bolnice u državi članici nisu obuhvaćene područjem primjene Direktive NIS i stoga nisu obvezne provoditi sigurnosne mjere koje iz nje proizlaze, dok je u drugoj državi članici gotovo svaka bolnica u zemlji obuhvaćena sigurnosnim zahtjevima za mrežne i informacijske sustave.

Što bi se trebalo postići?

U okviru preispitivanja sigurnosti mrežnih i informacijskih sustava predviđena su tri opća cilja:

1. **povećanje razine kiberotpornosti sveobuhvatnog skupa poduzeća koja posluju u Europskoj uniji u svim relevantnim sektorima** uspostavom pravila kojima se osigurava da su svi javni i privatni subjekti na cijelom unutarnjem tržištu, koji izvode važne funkcije za gospodarstvo i društvo u cjelini, obvezni poduzeti odgovarajuće kibersigurnosne mjere;
2. **smanjenje nedosljednosti u pogledu otpornosti na unutarnjem tržištu u sektorima koji su već obuhvaćeni Direktivom** daljnjim usklađivanjem (1) *de facto* područja primjene, (2) zahtjeva sigurnosti i izvješćivanja o incidentima, (3) odredaba kojima se uređuje nacionalni nadzor i provedba i (4) kapaciteta nadležnih tijela u državama članicama;
3. **poboljšanje stupnja zajedničke informiranosti o stanju i kolektivne sposobnosti pripreme i odgovora** poduzimanjem mjera za povećanje razine povjerenja među nadležnim tijelima, razmjenom veće količine informacija te utvrđivanjem pravila i postupaka u slučaju incidenta ili krize velikih razmjera.

Koja je dodana vrijednost djelovanja na razini EU-a (supsidijarnost)?

Otpornost u području kibersigurnosti u cijeloj Uniji ne može biti učinkovita ako joj se različito pristupa u okviru nacionalnih ili regionalnih izoliranih sustava. Taj je nedostatak riješen Direktivom NIS uspostavom okvira za sigurnost mrežnih i informacijskih sustava na nacionalnoj razini i na razini Unije. Međutim, tijekom njezina prenošenja i provedbe otkriveni su i inherentni nedostaci određenih odredaba ili pristupa, kao što je nejasno određivanje njezina područja primjene. Nadalje, pojavom krize uzrokovane bolešću COVID-19 europsko gospodarstvo postalo je ovisnije o mrežnim i informacijskim sustavima nego ikad prije, a sektori i usluge međusobno su sve povezaniji. Stoga je prvim periodičnim preispitivanjem Direktive NIS stvorena prilika za daljnje djelovanje EU-a. Intervencija EU-a koja nadilazi trenutačne

mjere Direktive NIS opravdana je uglavnom: i. prekograničnom prirodom problema; ii. potencijalom za djelovanje EU-a u cilju poboljšanja i olakšavanja učinkovitih nacionalnih politika; iii. doprinosom usklađenih i suradničkih mjera politike za sigurnost mrežnih i informacijskih sustava u cilju djelotvorne zaštite podataka i privatnosti.

B. Rješenja

Koje su opcije za postizanje ciljeva? Daje li se prednost određenoj opciji? Ako ne, zašto?

U procjeni učinka razmotrene su četiri opcije politike: (0) održavanje *statusa quo*; (1) nezakonodavne mjere za usklađivanje prenošenja; (2) ograničene izmjene Direktive NIS radi daljnjeg usklađivanja; (3) sustavne i strukturne izmjene Direktive NIS. Prva opcija odbačena je u ranoj fazi jer znatno ne odstupa od *statusa quo*. U procjeni učinka zaključuje se da je **najpoželjnija treća opcija** (tj. **sustavne i strukturne izmjene okvira za sigurnost mrežnih i informacijskih sustava**) jer bi se njome predvidjela temeljitija promjena pristupa prema obuhvaćanju šireg segmenta gospodarstava diljem Unije, ali uz usmjeravanje nadzora na razmjerno velika i ključna poduzeća, uz jasno utvrđivanje područja primjene. Njome bi se usto pojednostavnile i dodatno uskladile obveze poduzeća povezane sa sigurnošću, stvorilo djelotvornije okruženje za operativne aspekte, uspostavila jasna osnova za zajedničke obveze i odgovornost relevantnih aktera te potaknula razmjena informacija.

Koja su stajališta različitih dionika? Tko podržava koju opciju?

Većina nadležnih tijela i poduzeća podržala je reviziju Direktive NIS. Tijekom nekoliko savjetovanja naveli su da bi revidiranom Direktivom NIS trebalo obuhvatiti dodatne (pod)sektore te uskladiti ili racionalizirati daljnje sigurnosne mjere i obveze izvješćivanja. Dionici su također izrazili potporu novim konceptima ili mjerama povezanima s politikom koji su samo dio najpoželjnije mogućnosti (npr. politike sigurnosti lanca opskrbe, institucionalizacija operativnog okvira EU-a za upravljanje krizama).

C. Učinci najpoželjnije opcije

Koje su prednosti najpoželjnije opcije (ako takve opcije nema, prednosti glavnih opcija)?

Najpoželjnija opcija donijela bi znatne koristi: procjene izrađene na temelju ekonomskog modeliranja razvijenog u okviru popratne studije za preispitivanje sigurnosti mrežnih i informacijskih sustava upućuju na to da bi najpoželjnija opcija mogla dovesti do smanjenja troškova kiberincidenata za 11,3 milijarde EUR.

Sektorsko područje primjene znatno bi se proširilo okvirom za sigurnost mrežnih i informacijskih sustava, no uz navedene koristi, opterećenje koje bi moglo nastati zbog zahtjeva za sigurnost mrežnih i informacijskih sustava, posebno iz perspektive nadzora, uravnotežilo bi se za nove subjekte koji će biti obuhvaćeni tim okvirom, kao i za nadležna tijela. Razlog je tome taj što bi se novim okvirom za sigurnost mrežnih i informacijskih sustava uspostavio dvorazinski pristup, s naglaskom na velikim i ključnim subjektima, i razlikovanje sustava nadzora kojim bi se omogućio samo *ex post* nadzor (tj. reaktivan i bez opće obveze sustavnog dokumentiranja usklađenosti) za velik broj tih subjekata, posebno onih koji se smatraju „važnima”, ali nisu „ključni”.

Općenito, najpoželjnija opcija politike dovela bi do učinkovitih kompromisa i sinergija, uz iskorištavanje najboljeg potencijala svih analiziranih opcija politike kako bi se osigurala veća i stabilna razina kiberotpornosti ključnih subjekata diljem Unije, što bi u konačnici dovelo do uštede troškova za poduzeća i društvo.

Koji su troškovi najpoželjnije opcije (ako takve opcije nema, troškovi glavnih opcija)?

Najpoželjnija opcija politike dovela bi do određenih troškova usklađivanja i provedbe za relevantna tijela država članica (procijenjeno je ukupno povećanje od oko 20–30 % sredstava). Međutim, novi bi okvir donio i znatne koristi zahvaljujući boljem pregledu i interakciji s ključnim poduzećima, pojačanoj prekograničnoj operativnoj suradnji te mehanizmima uzajamne pomoći i istorazinskog ocjenjivanja. To bi dovelo do sveukupnog povećanja kibersigurnosnih kapaciteta u državama članicama.

Kad je riječ o poduzećima koja bi bila obuhvaćena područjem primjene okvira za sigurnost mrežnih i informacijskih sustava, procjenjuje se da će potrebno povećanje iznositi najviše 22 % njihovih trenutačnih rashoda za sigurnost IKT-a tijekom prvih godina nakon uvođenja novog okvira za sigurnost mrežnih i informacijskih sustava (to bi iznosilo 12 % za poduzeća koja su već obuhvaćena područjem primjene postojeće Direktive NIS). Međutim, to prosječno povećanje rashoda za sigurnost IKT-a dovelo bi do razmjerne koristi od takvih ulaganja, posebno zbog znatnog smanjenja troškova kiberincidenata (koji su procijenjeni na 11,3 milijarde EUR tijekom deset godina).

Koji su učinci na MSP-ove i konkurentnost?

U okviru najpoželjnije opcije mala i mikropoduzeća bila bi izuzeta iz područja primjene okvira za sigurnost mrežnih i informacijskih sustava. Kad je riječ o srednjim poduzećima, može se očekivati povećanje razine rashoda za sigurnost IKT-a u prvim godinama nakon uvođenja novog okvira za sigurnost mrežnih i informacijskih sustava. Istodobno bi se povećanjem razine sigurnosnih zahtjeva za te subjekte potaknulo povećanje njihovih kibersigurnosnih kapaciteta i poboljšalo njihovo upravljanje rizicima u području IKT-a.

Hoće li to znatno utjecati na nacionalne proračune i uprave?

To bi utjecalo na nacionalne proračune i uprave: procjenjuje se da bi se povećanje od približno 20–30 % sredstava moglo očekivati u kratkom i srednjem roku.

Hoće li biti drugih znatnih učinaka?

Ne očekuju se drugi znatni negativni učinci. Očekuje se da će najpoželjnija opcija politike za posljedicu imati robusnije kibersigurnosne kapacitete te zahvaljujući tome znatnije umanjiti količinu i ozbiljnost incidenata, uključujući povrede podataka. Vjerojatno će pozitivno utjecati i na osiguravanje ravnopravnih uvjeta u svim državama članicama za sve subjekte obuhvaćene područjem primjene okvira za sigurnost mrežnih i informacijskih sustava te na smanjenje asimetričnosti informacija u području kibersigurnosti.

Proporcionalnost

Najpoželjnija opcija ne prelazi okvire onoga što je potrebno za zadovoljavajuće ispunjenje posebnih ciljeva. Predviđeno usklađivanje i racionalizacija sigurnosnih mjera i obveza izvješćivanja odnose se na zahtjeve država članica i poduzeća za poboljšanje postojećeg okvira.

D. Daljnje mjere

Kad će se predložene mjere preispitati?

Pravni instrument prvi bi se put preispitao 54 mjeseca od stupanja na snagu. Komisija bi Europskom parlamentu i Vijeću dostavila izvješće o preispitivanju. Preispitivanje bi se pripremiti uz potporu ENISA-e i skupine za suradnju.